ASA 8.2:使用ASDM通過nat、global、static和access-list命令進行埠重定向（轉發）

目錄

簡介

本檔案介紹使用ASDM在思科調適型安全裝置(ASA)上執行連線埠重新導向的方式。它處理通過ASA的流量的訪問控制以及轉換規則的工作方式。

必要條件

需求

思科建議您瞭解以下主題：

- NAT概述
- PIX/ASA 7.X:連線埠重新導向

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5500系列ASA版本8.2
- Cisco ASDM版本6.3

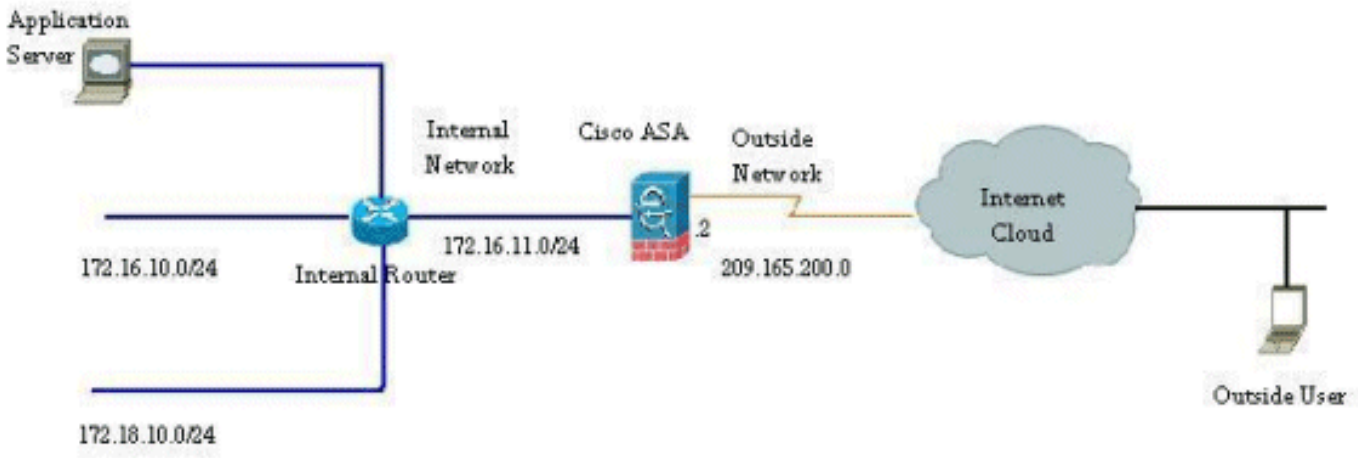
注意：此配置僅在Cisco ASA軟體版本8.0到8.2之間運行良好，因為NAT功能沒有重大更改。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

網路圖表

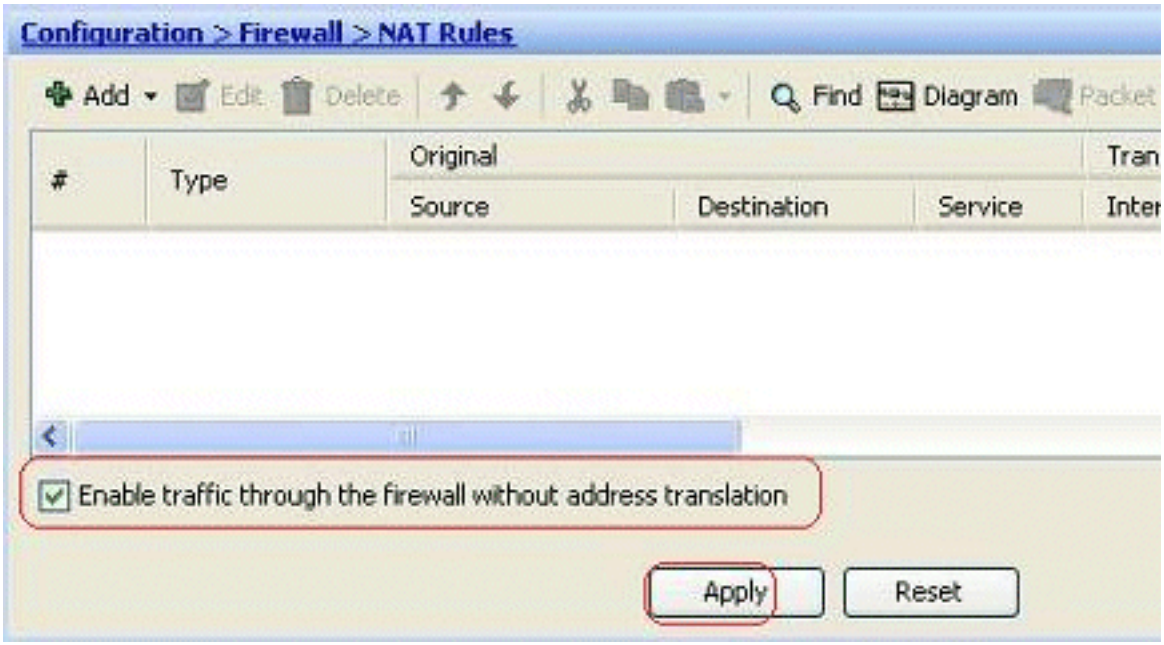


此配置中使用的IP編址方案在Internet上不能合法路由。這些地址是在實驗室環境中使用的RFC 1918地址。

允許出站訪問

出站訪問描述從較高安全級別介面到較低安全級別介面的連線。這包括從內部到外部、從內部到非軍事區(DMZ)以及從非軍事區到外部的連線。只要連線源介面的安全級別高於目標介面，這還可以包括從一個DMZ到另一個DMZ的連線。

沒有配置轉換規則，任何連線都無法通過安全裝置。此功能稱為nat-control。此處顯示的影象說明了如何通過ASDM禁用此功能，以便允許通過ASA的連線而無需任何地址轉換。但是，如果您配置了任何轉換規則，則禁用此功能不會對所有流量保持有效，您需要明確排除網路的地址轉換。

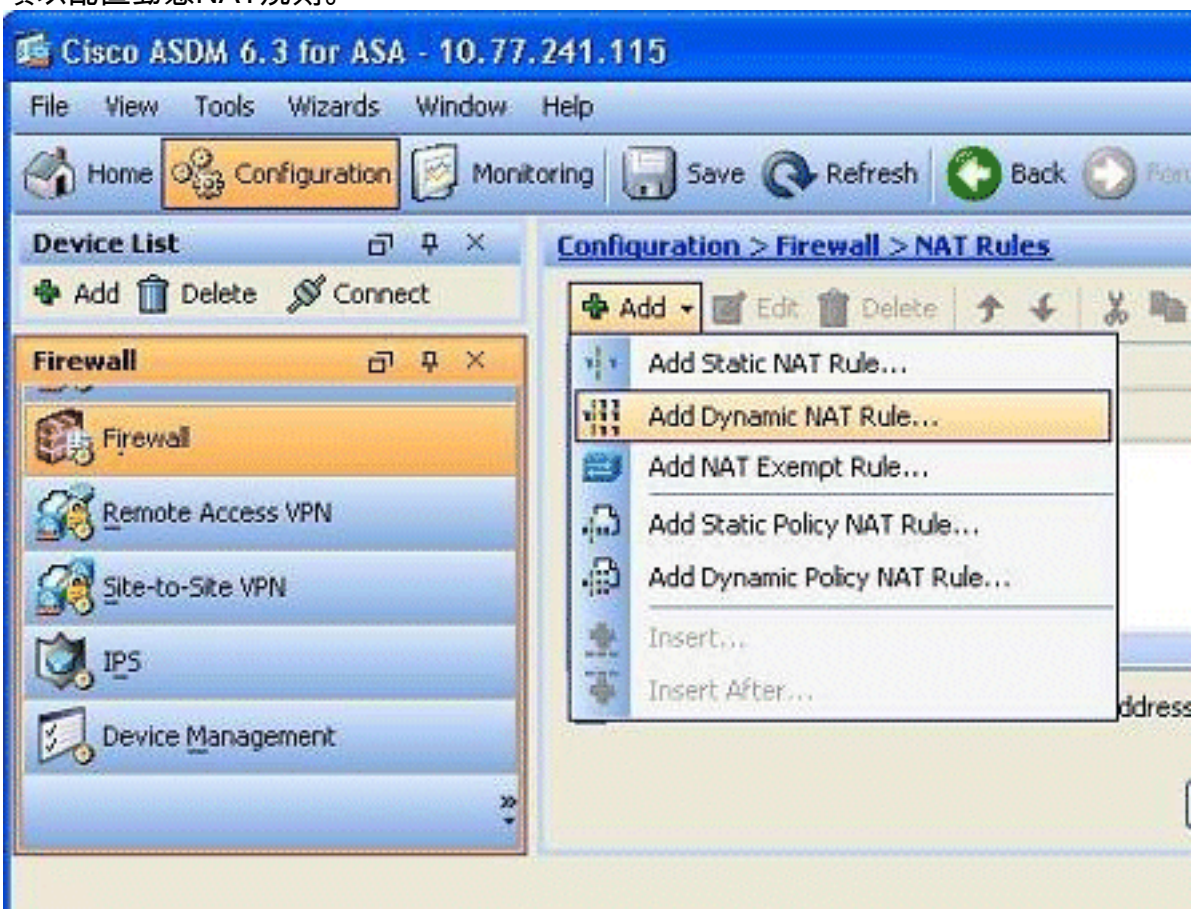


允許內部主機通過NAT訪問外部網路

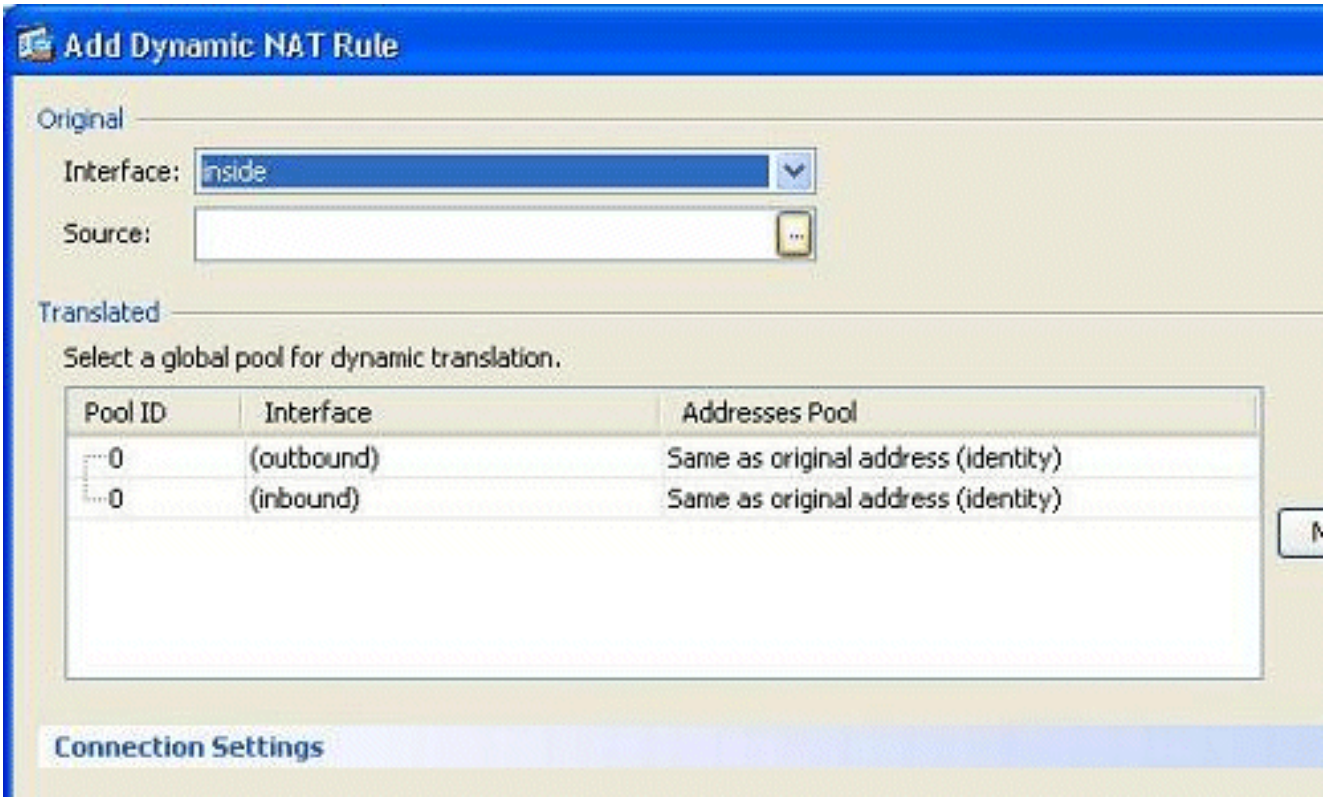
您可以通過配置動態NAT規則來允許一組內部主機/網路訪問外部世界。為此，您需要選擇要授予訪問許可權的主機/網路的實際地址，然後必須將其對映到已轉換的IP地址池。

完成以下步驟，以允許內部主機通過NAT訪問外部網路：

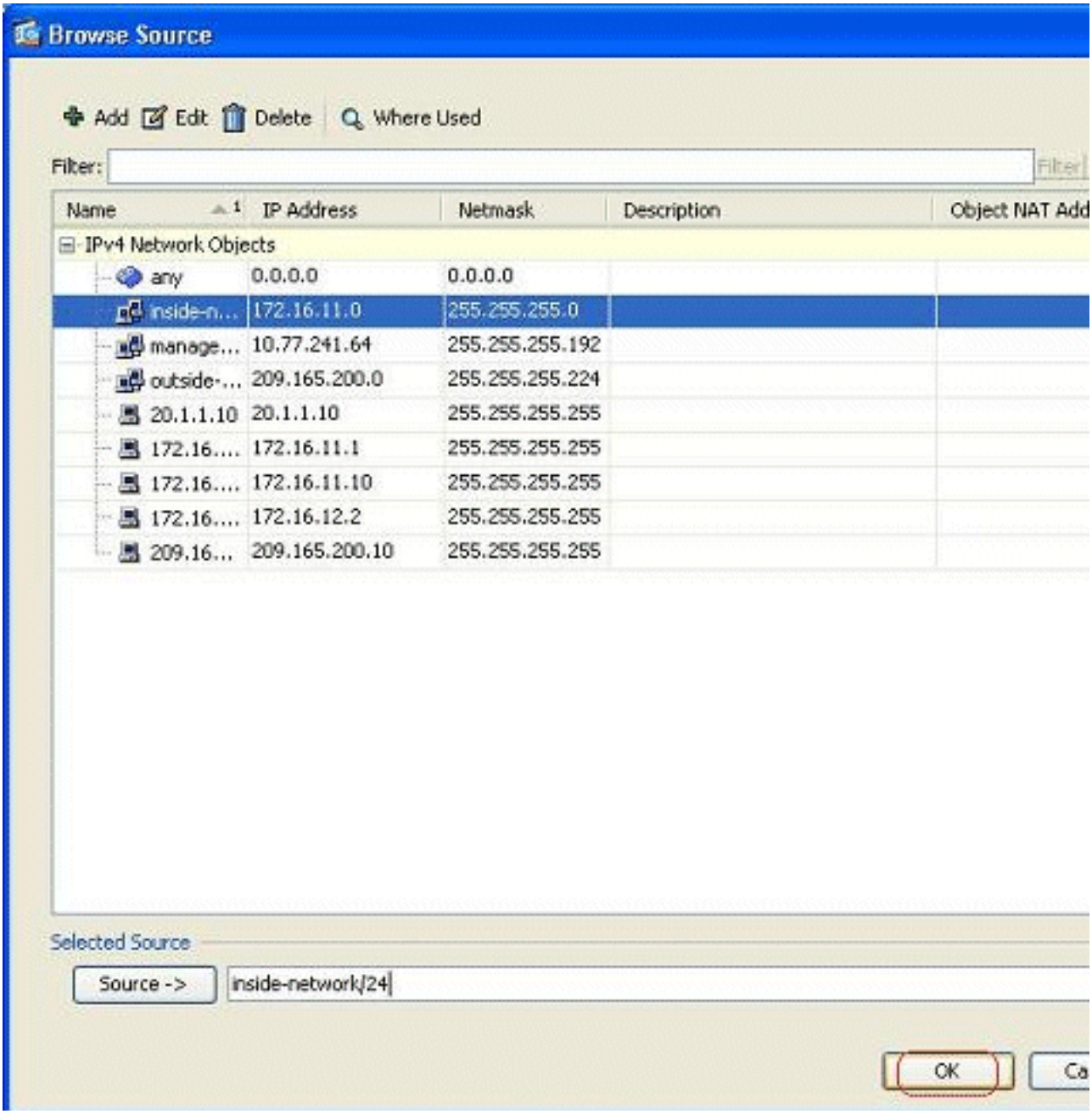
1. 轉至Configuration > **Firewall** > **NAT Rules**，按一下**Add**，然後選擇Add Dynamic NAT Rule選項以配置動態NAT規則。



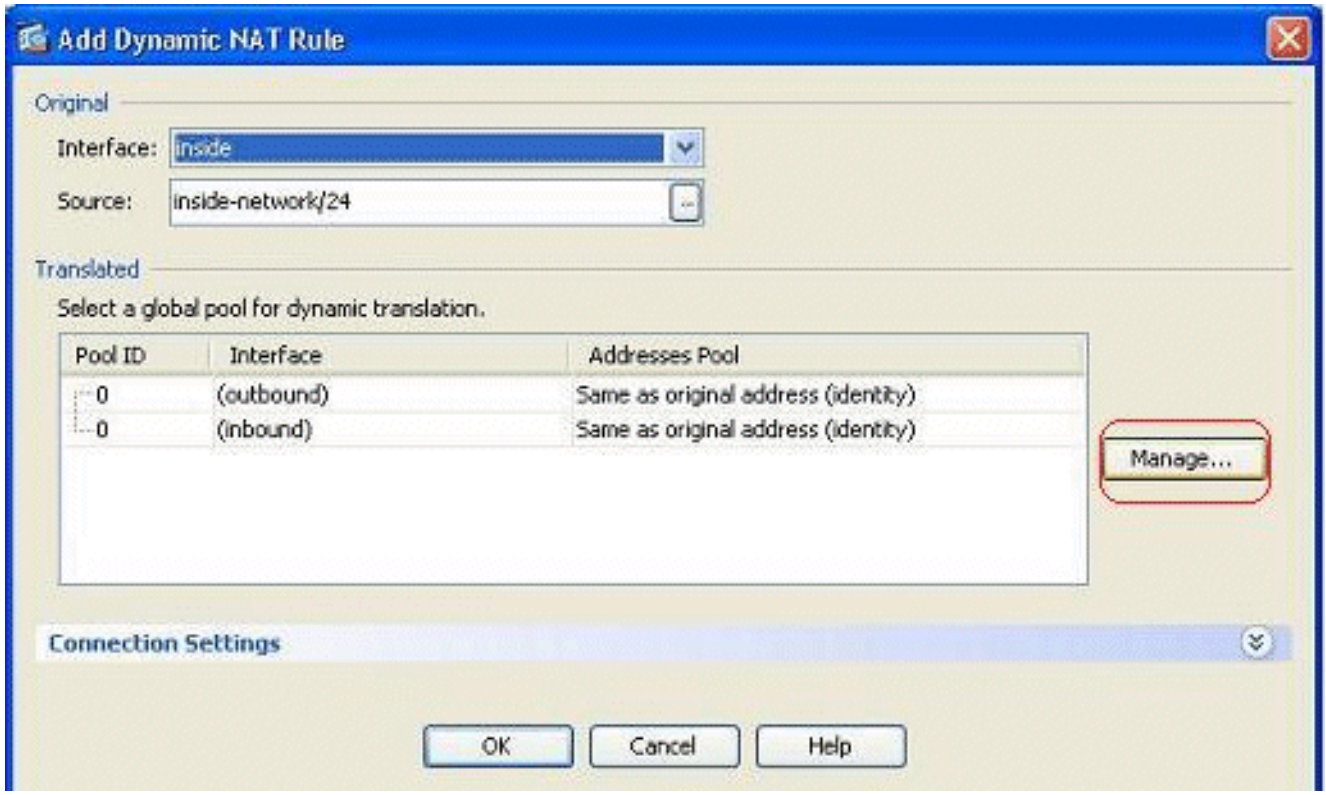
2. 選擇實際主機所連線的介面的名稱。使用**Source**欄位中的**Details**按鈕選擇主機/網路的實際IP地址。



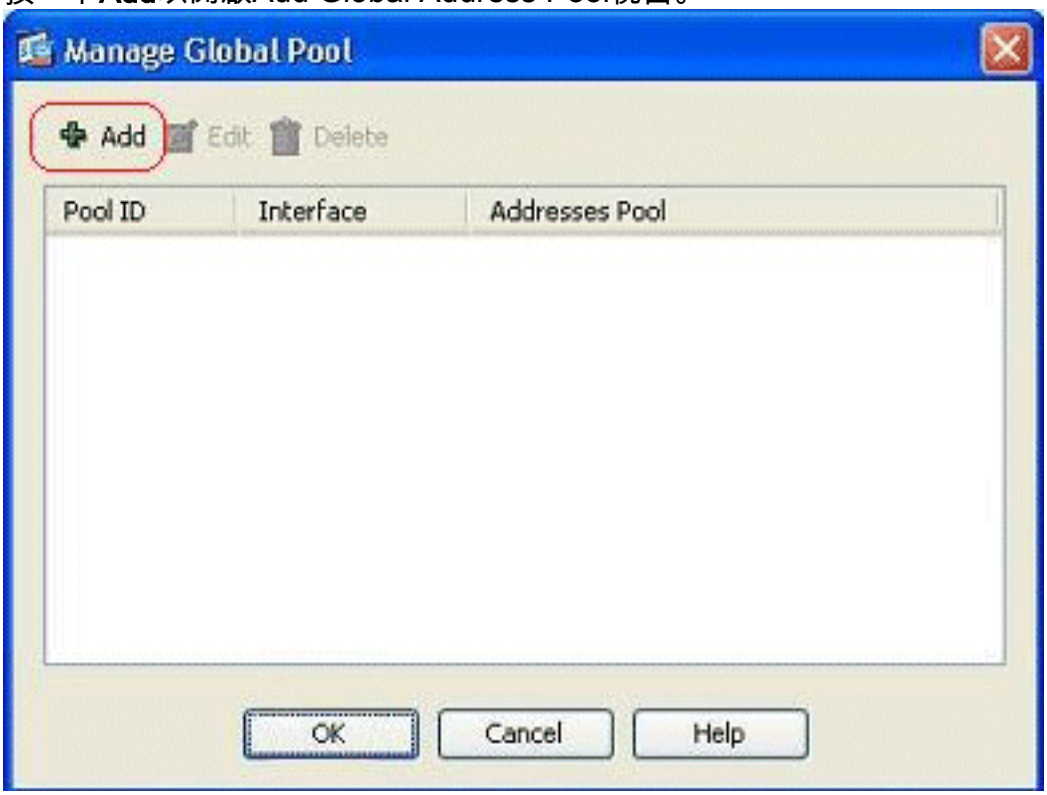
3. 在本示例中，已選擇*整個內部*網路。按一下**OK**以完成選擇。



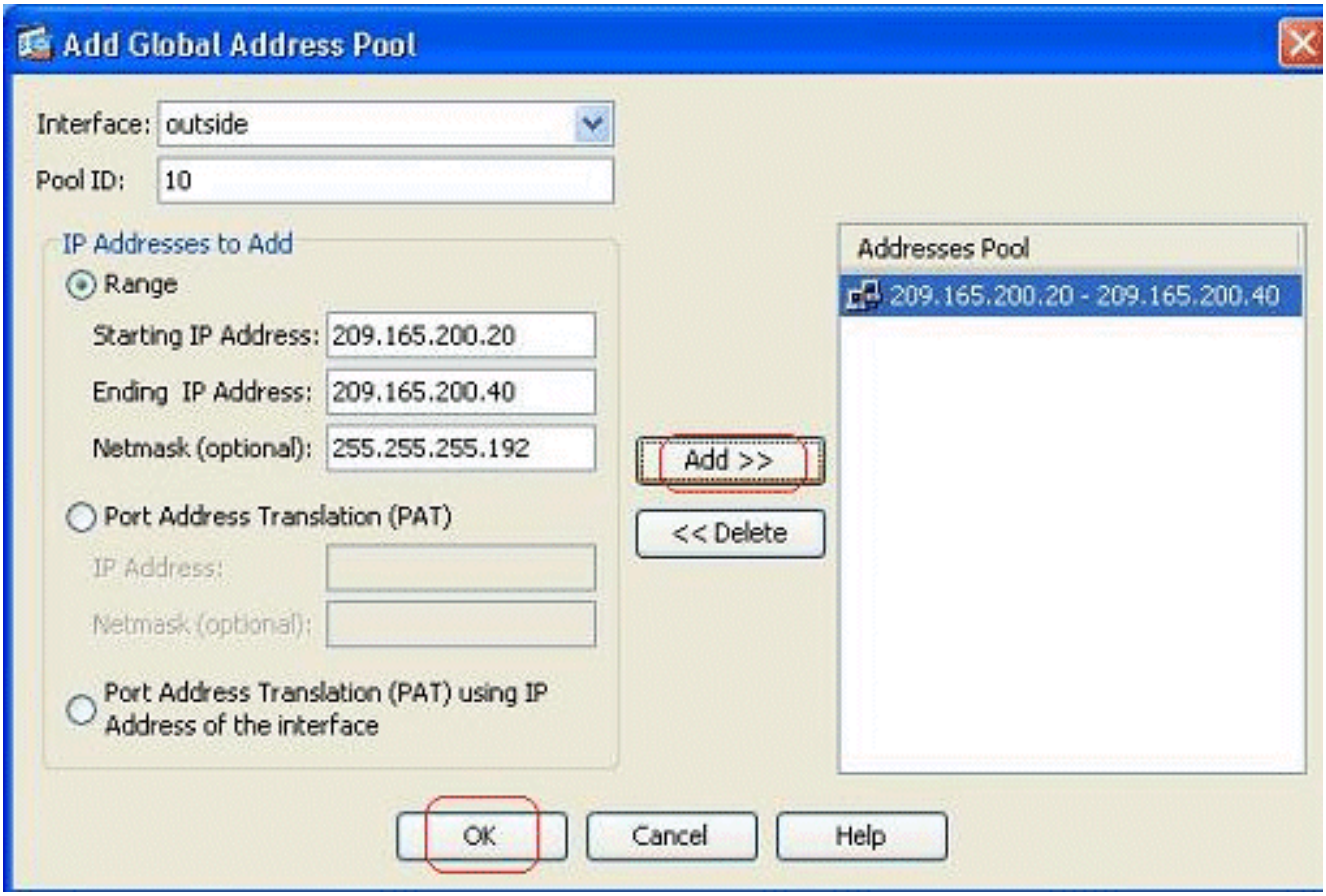
4. 按一下**Manage**以選擇實際網路將對映到的IP地址池。



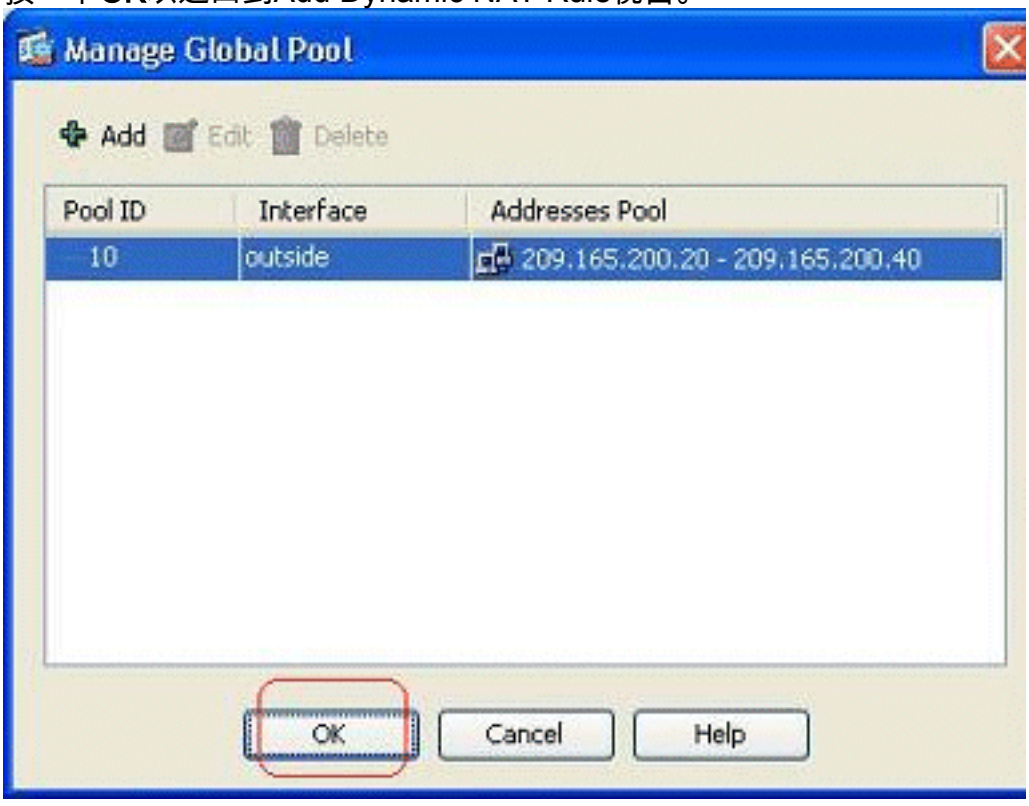
5. 按一下**Add**以開啟Add Global Address Pool視窗。



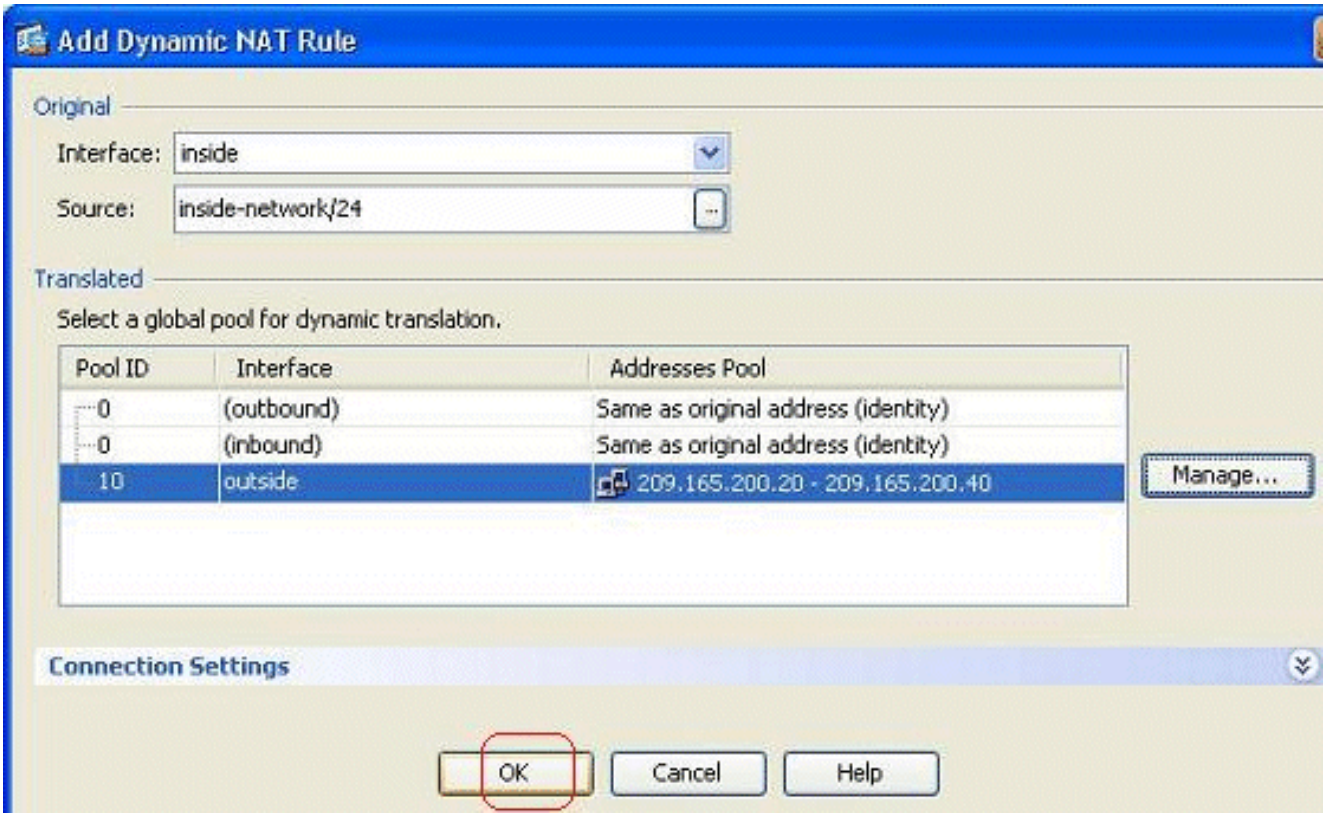
6. 選擇**Range**選項並指定Starting and Ending IP Addresses以及輸出介面。此外，請指定唯一池ID並按一下**Add**以將其新增到地址池。按一下**OK**以返回到「管理全域性池」視窗。



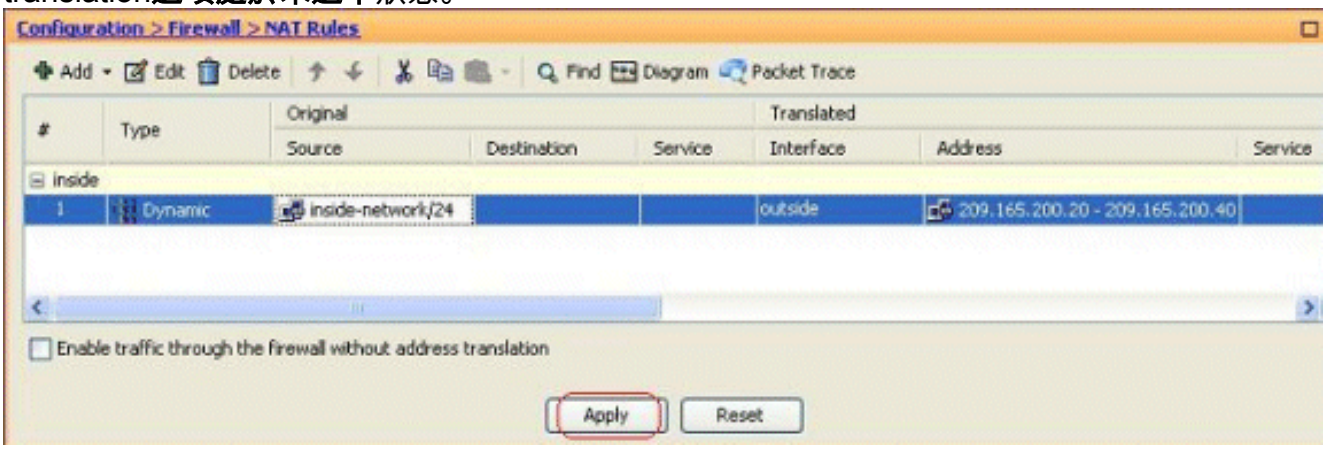
7. 按一下**OK**以返回到Add Dynamic NAT Rule視窗。



8. 按一下**OK**以完成動態NAT規則配置。



9. 按一下**Apply**以使更改生效。**注意：**Enable traffic through the firewall without address translation**選項處於未選中**狀態。



這是此ASDM配置的等效的CLI輸出：

```
nat-control
global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192
nat (inside) 10 172.16.11.0 255.255.255.0
```

根據此配置，172.16.11.0網路中的主機將轉換為NAT池209.165.200.20-209.165.200.40中的任何IP地址。在這裡，NAT池ID非常重要。可以將相同的NAT池分配給另一個內部/dmz網路。如果對映池的地址少於實際組，則當流量大於預期時，地址可能會用盡。因此，您可以嘗試實施PAT，也可以嘗試編輯現有地址池以對其進行擴展。

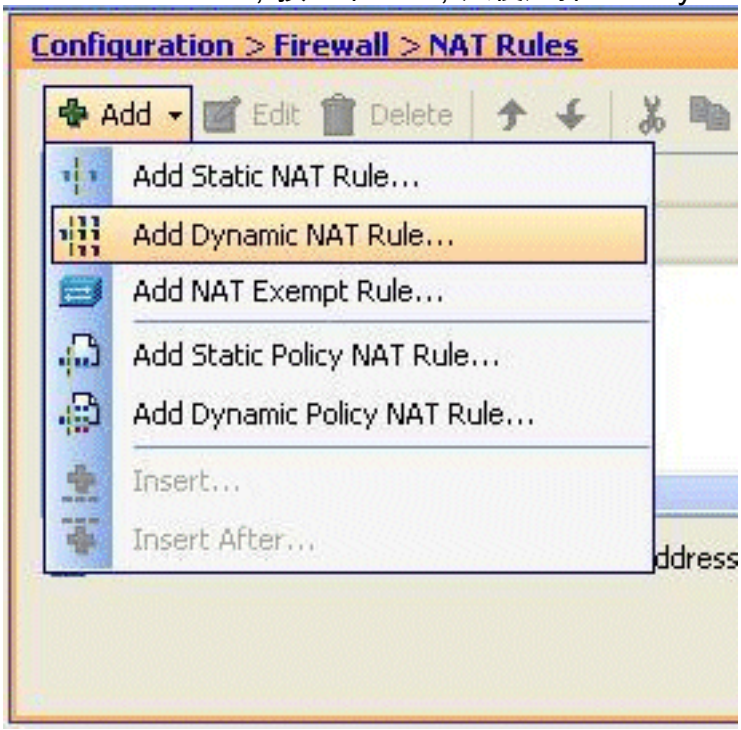
注意：在對現有轉換規則進行任何修改時，請注意，需要使用clear xlate**命令才能使這些修改生效。**否則，先前的現有連線將保留在連線表中，直到它們超時。使用**clear xlate**命令時要小心，因為它會立即終止現有連線。

允許內部主機通過PAT訪問外部網路

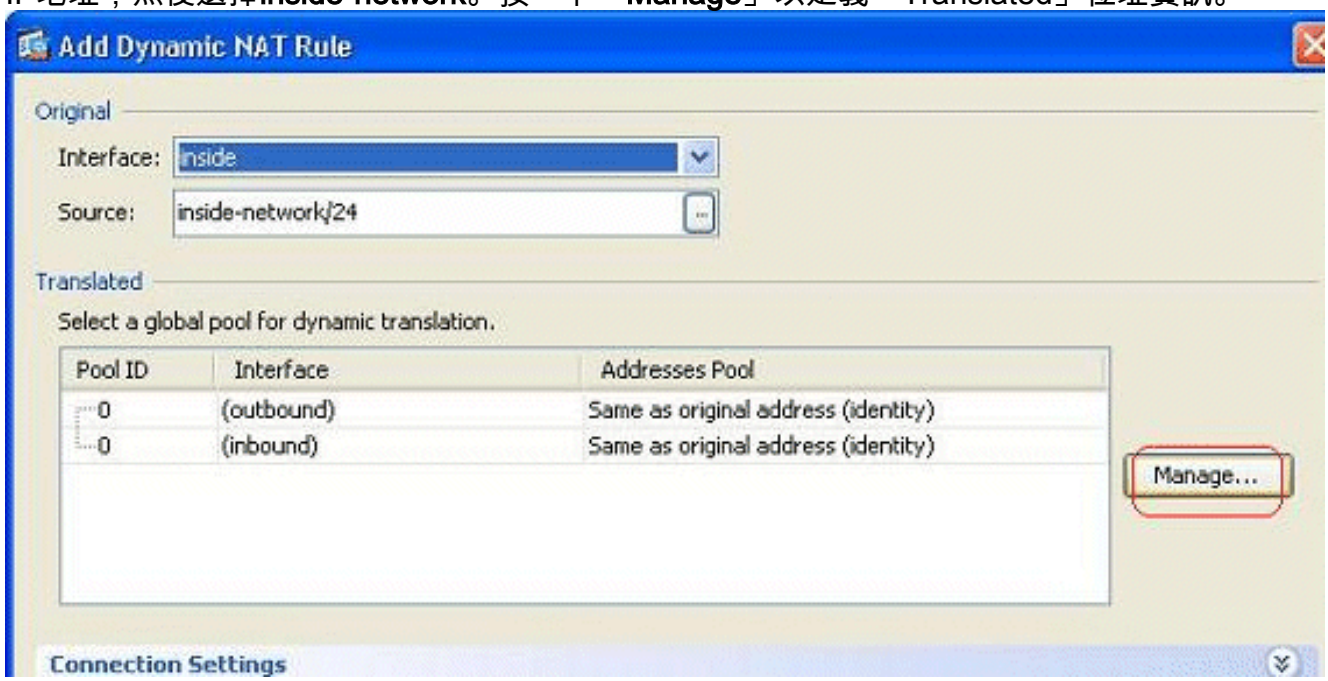
如果希望內部主機共用一個公共地址進行轉換，請使用PAT。如果**global**語句指定一個地址，則該地址為埠轉換。ASA允許每個介面進行一個埠轉換，該轉換支援最多65,535個活動**xlate**對象到單個全域性地址。

完成以下步驟，以允許內部主機使用PAT訪問外部網路：

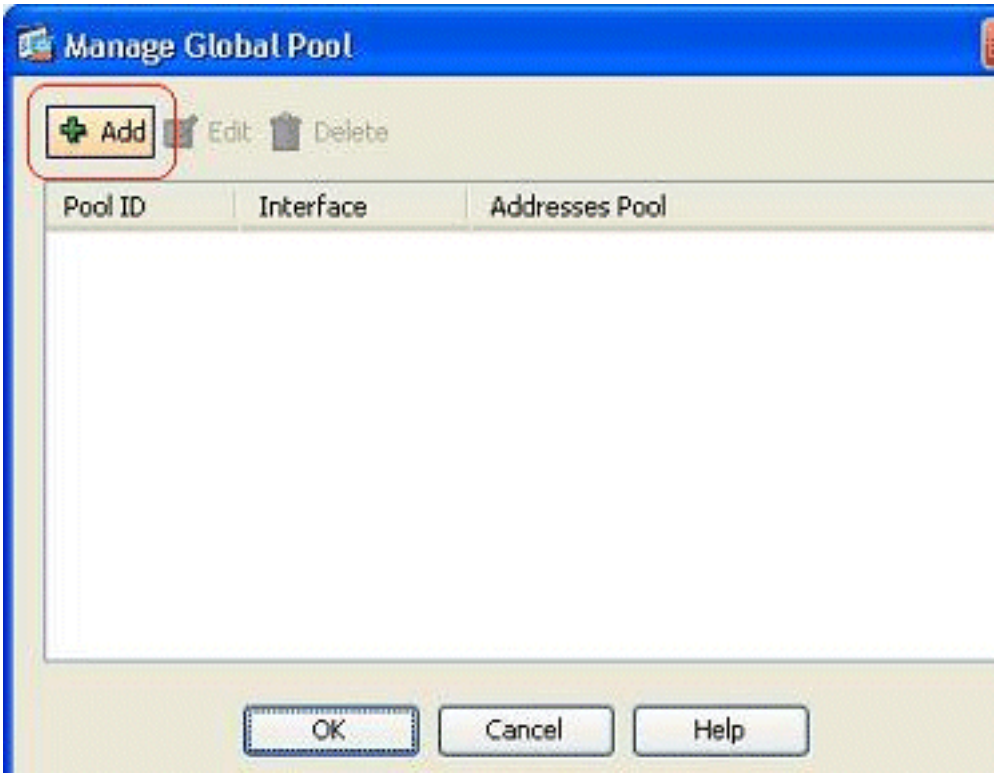
1. 轉至Configuration > **Firewall** > **NAT Rules**，按一下**Add**，然後選擇Add Dynamic NAT Rule選項以配置動態NAT規則。



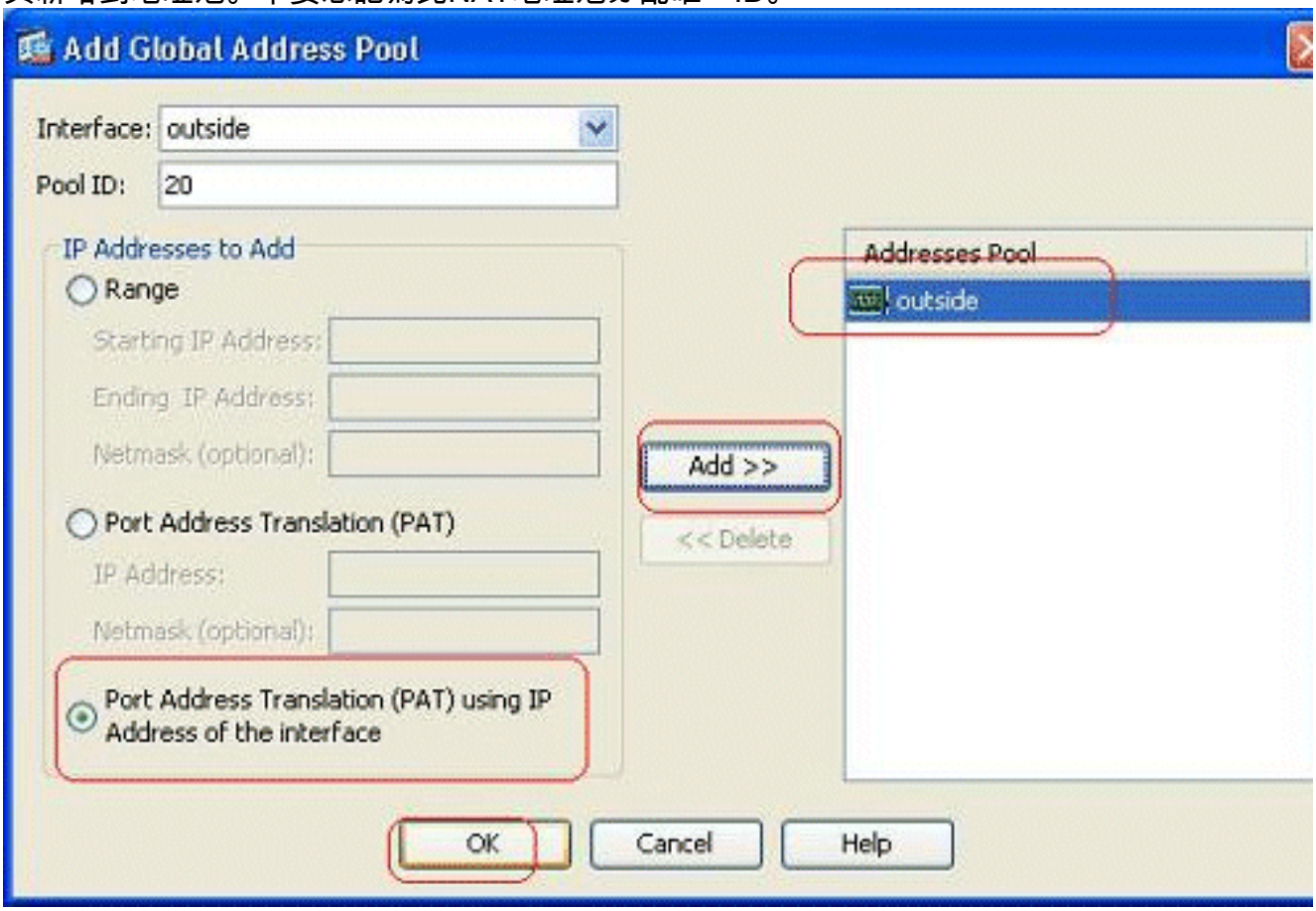
2. 選擇實際主機所連線的介面的名稱。使用**Source**欄位中的**Details**按鈕選擇主機/網路的實際IP地址，然後選擇**inside-network**。按一下「**Manage**」以定義「Translated」位址資訊。



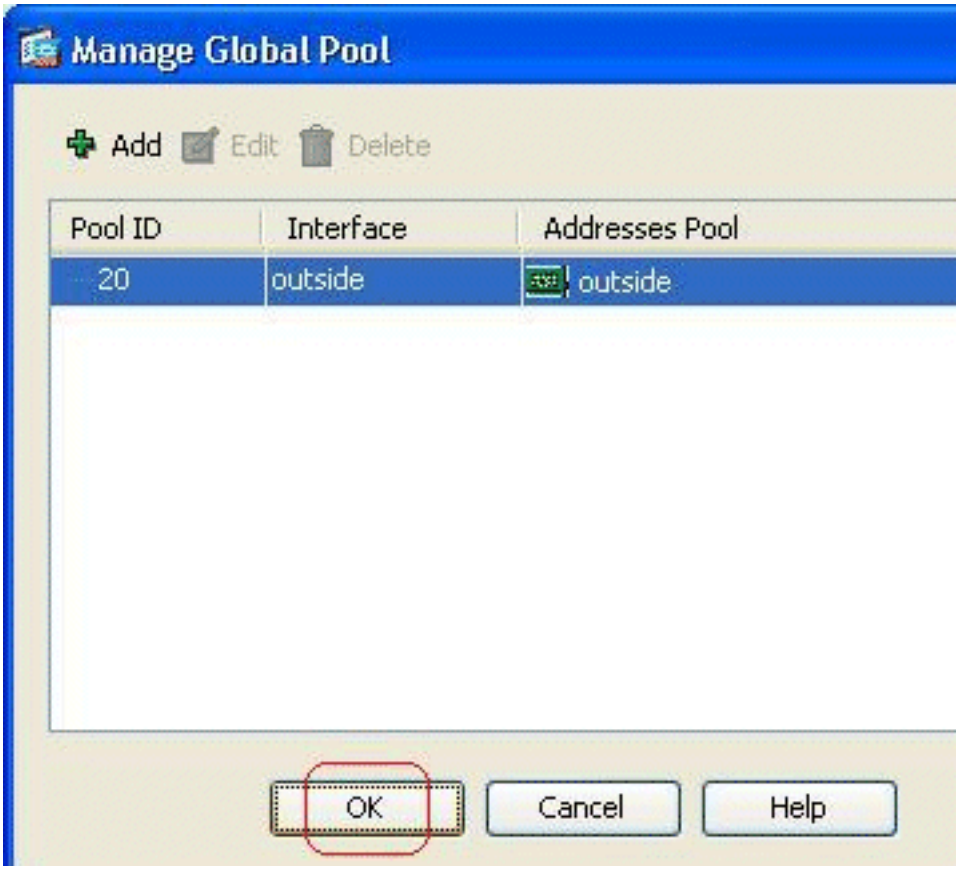
3. 按一下「**Add**」。



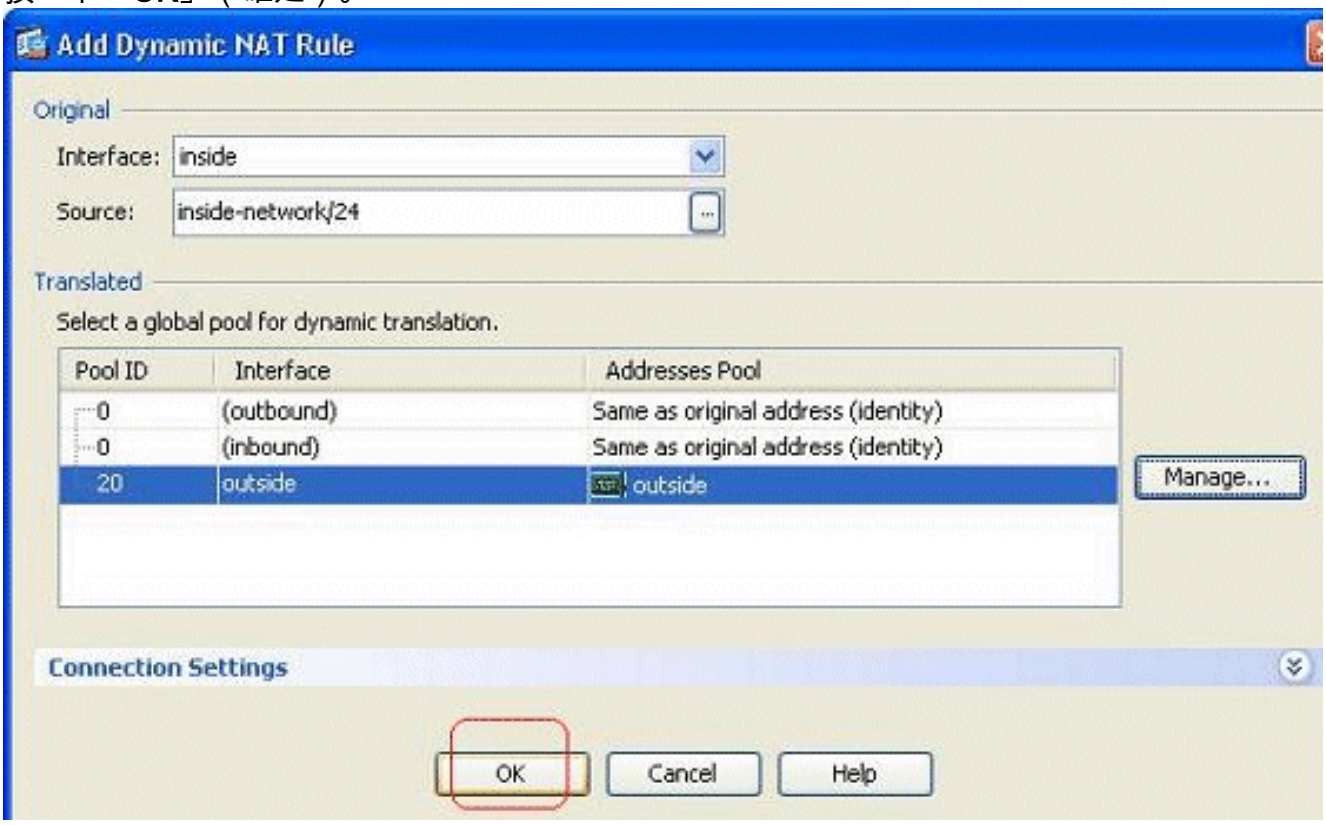
4. 選擇**Port Address Translation(PAT)using IP address of the interface**選項，然後按一下**Add**將其新增到地址池。不要忘記為此NAT地址池分配唯一ID。



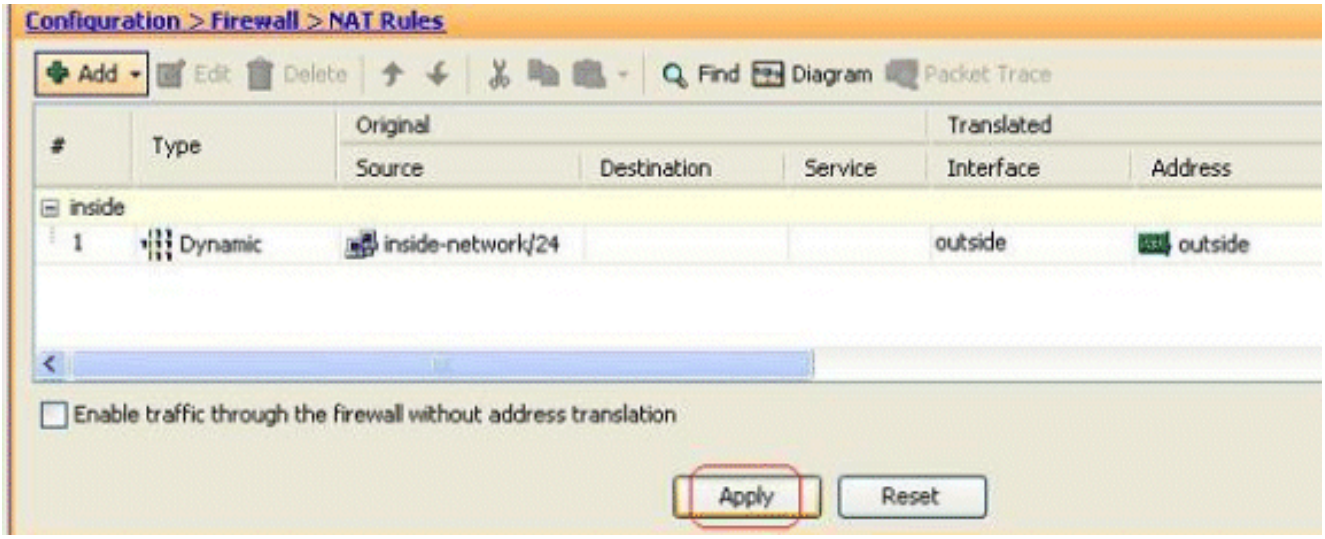
5. 此處顯示的是已配置的地址池，外部介面是該池中唯一可用的地址。按一下**OK**以返回到Add Dynamic NAT Rule視窗。



6. 按一下「**OK**」（確定）。



7. 此處的Configuration > Firewall > NAT Rules窗格中顯示了配置的動態NAT規則。



這是此PAT配置的等效的CLI輸出：

```
global (outside) 20 interface
nat (inside) 20 172.16.11.0 255.255.255.0
```

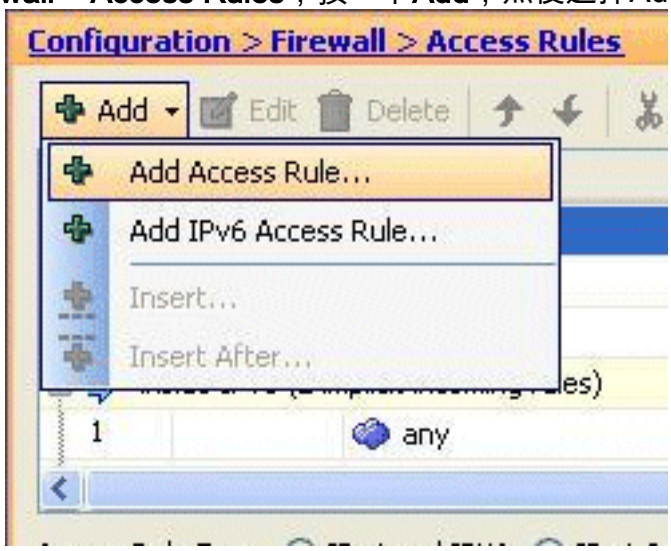
限制內部主機訪問外部網路

如果未定義訪問規則，則來自較高安全介面的使用者可以訪問與較低安全介面關聯的任何資源。要限制特定使用者訪問某些資源，請在ASDM中使用訪問規則。本示例說明如何允許單個使用者訪問外部資源（使用FTP、SMTP、POP3、HTTPS和WWW）並限制所有其他使用者訪問外部資源。

注意：每個訪問清單的結尾都有一個「隱式拒絕」規則。

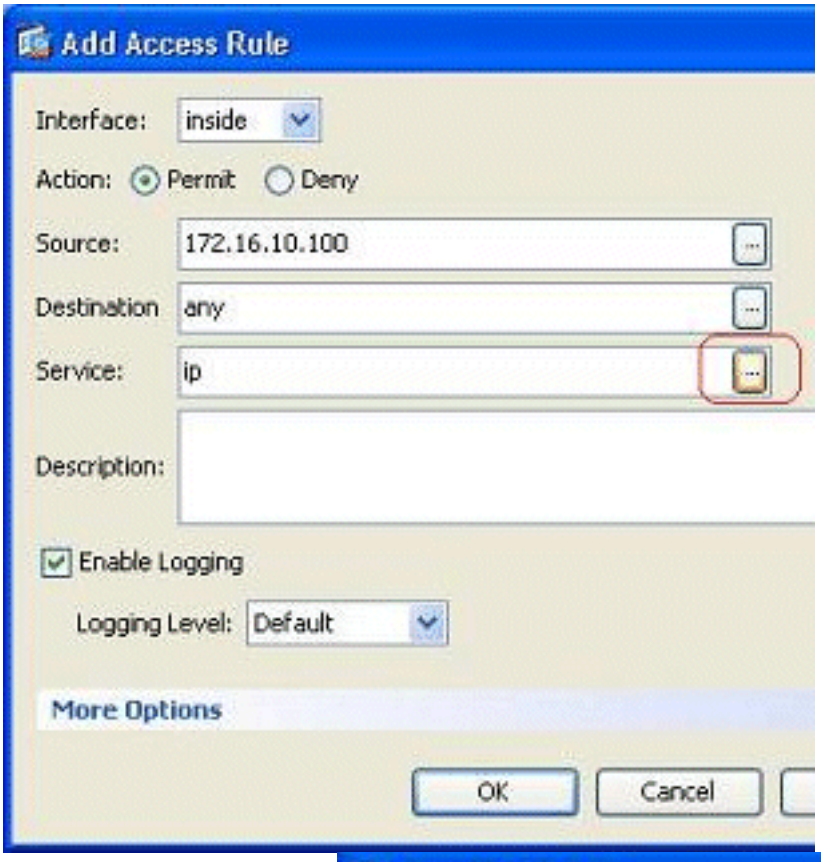
請完成以下步驟：

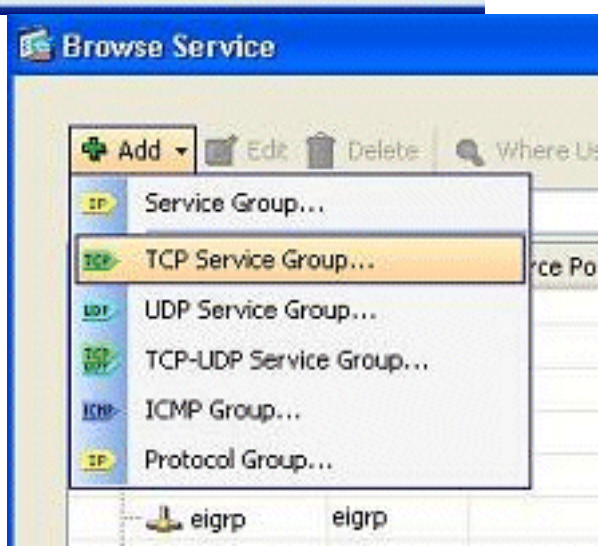
1. 轉至Configuration > **Firewall > Access Rules**，按一下**Add**，然後選擇Add Access Rule選項以建立新的訪問清單條目。



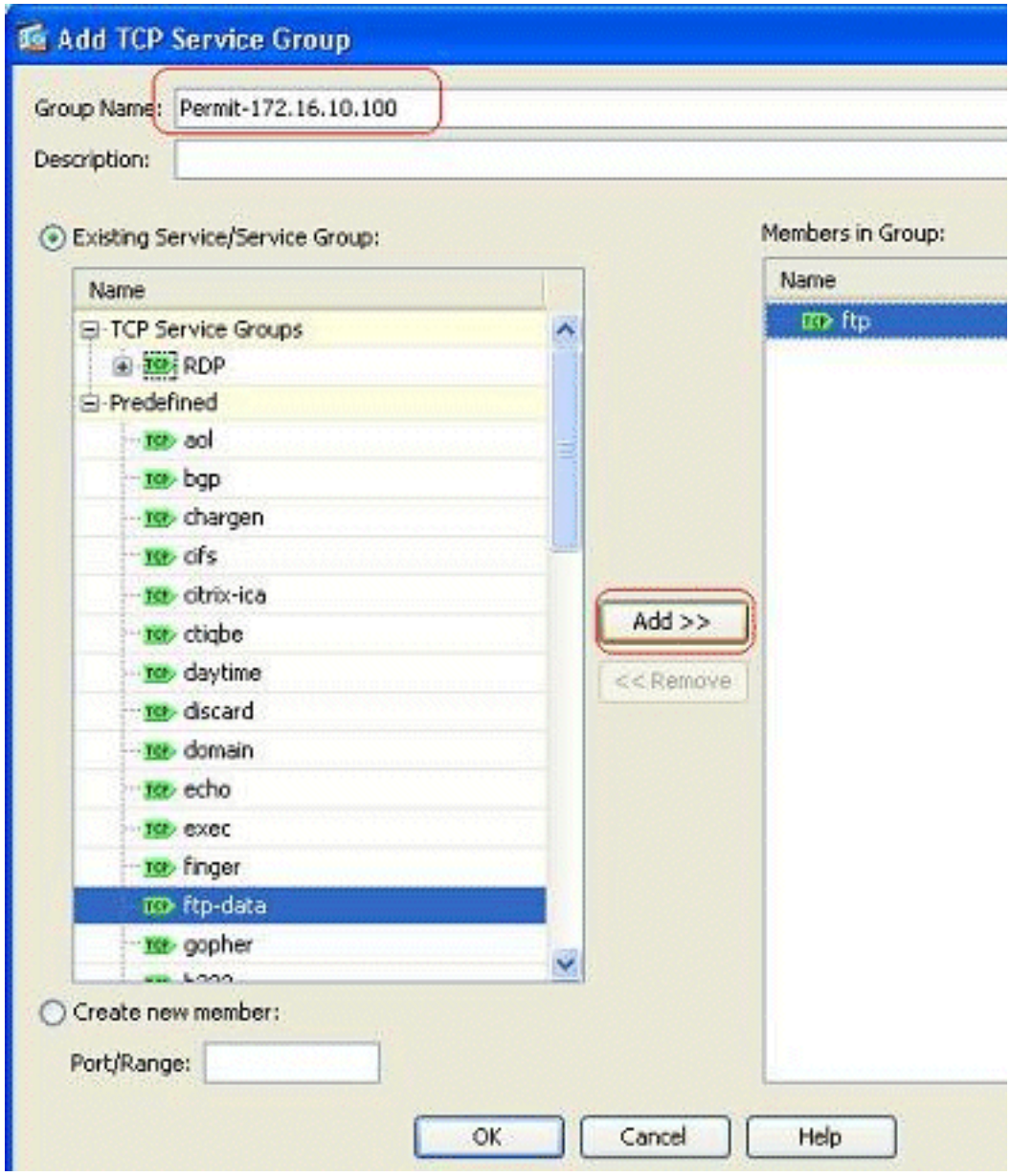
2. 在**Source**欄位中選擇要允許的源IP地址。選擇**any**作為Destination（目標）、**inside**作為Interface（介面），然後選擇**Permit**（操作）。最後，按一下Service欄位中的**Details**按鈕，為

所需埠建立TCP服務組。

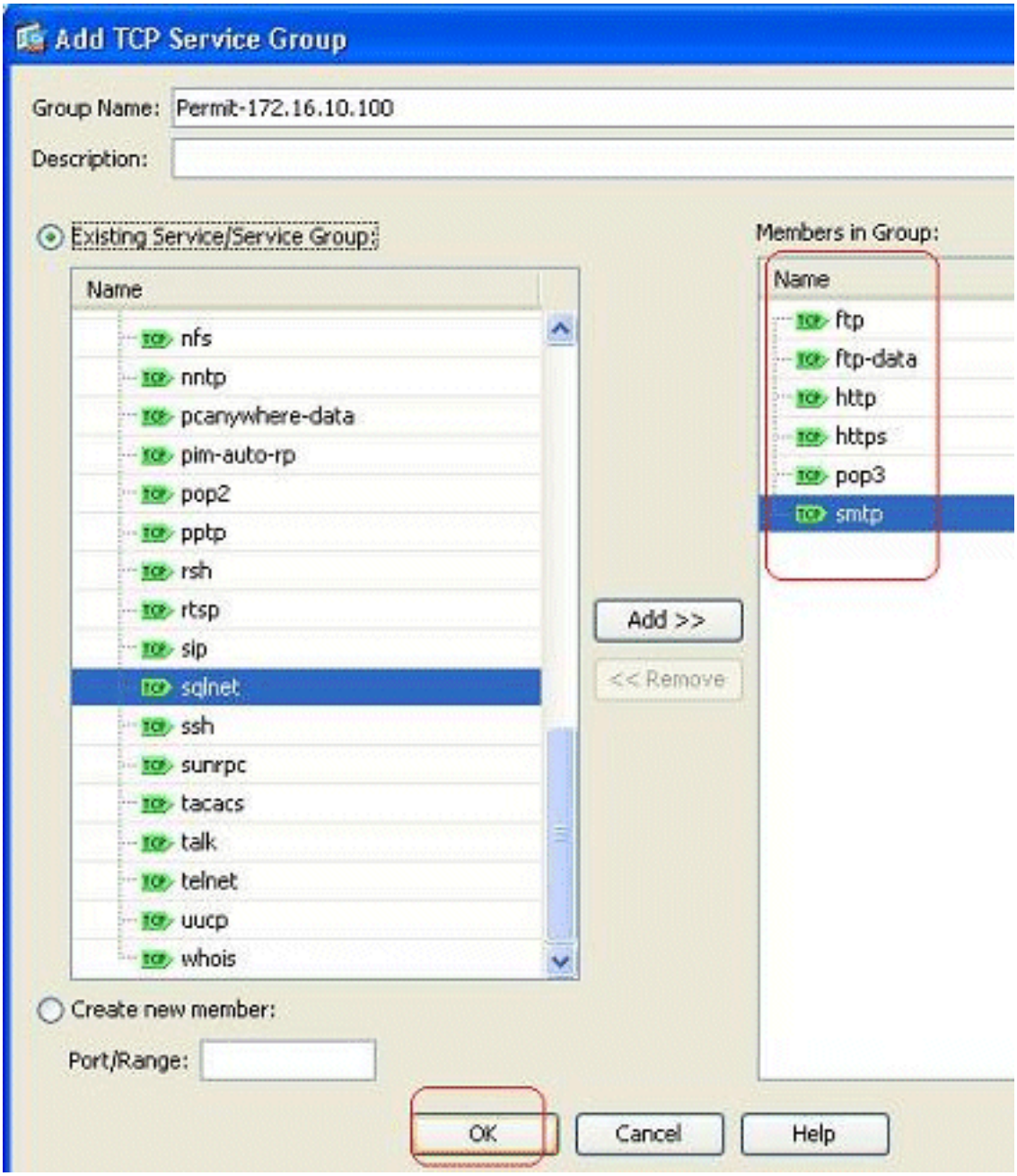




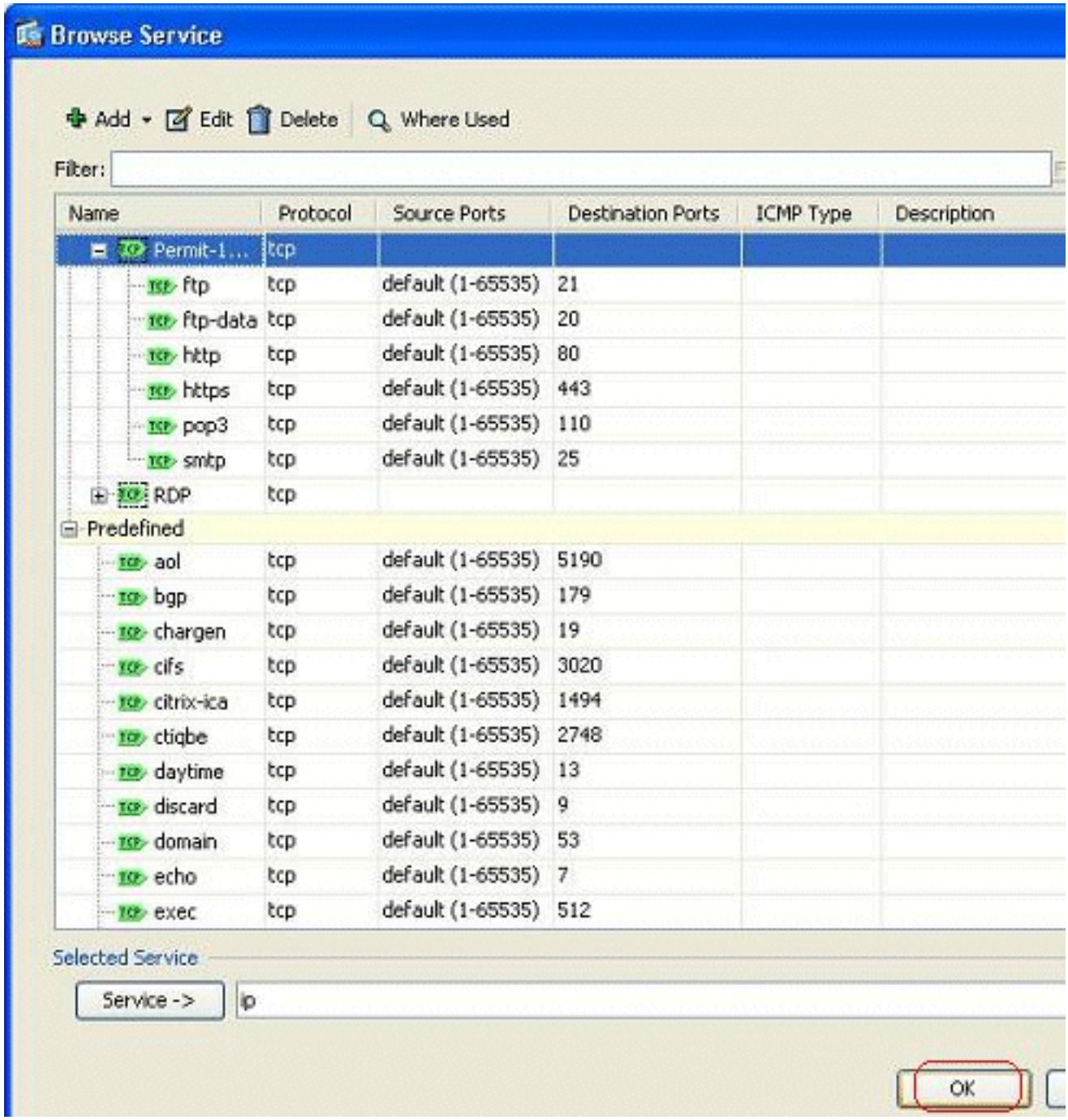
3. 按一下**Add**，然後選擇**TCP Service Group**選項。
4. 輸入此組的名稱。選擇每個所需的埠，然後按一下**Add**以將其移動到「組中的成員」欄位。

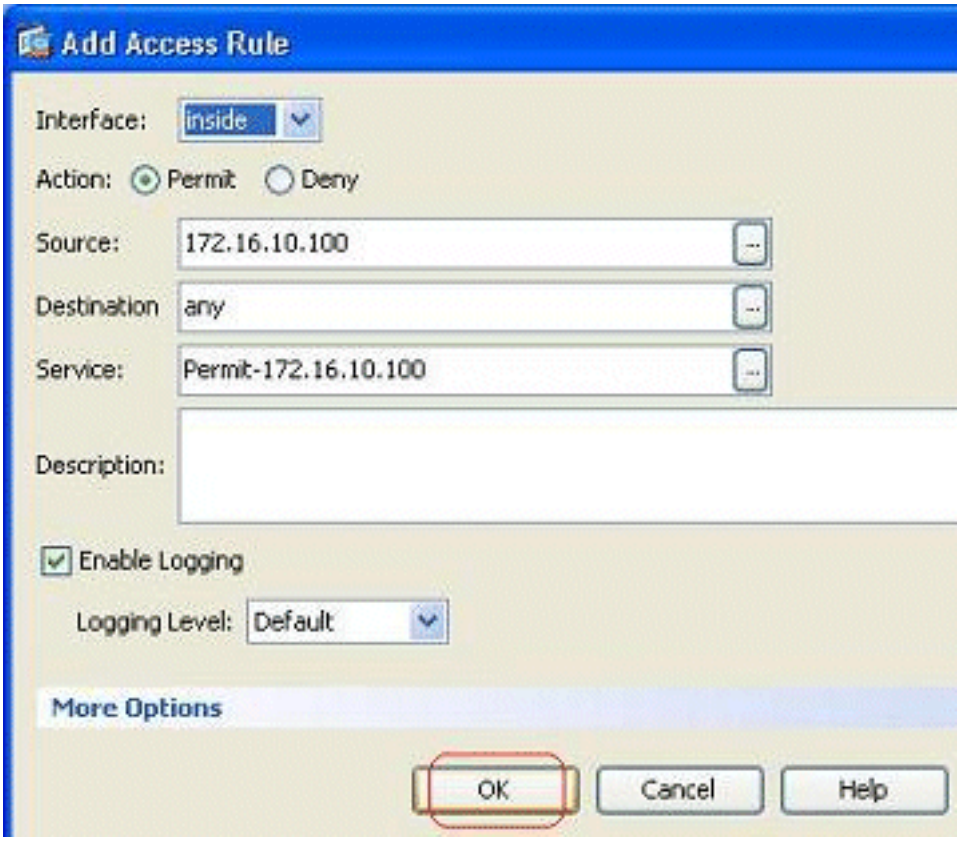


5. 您應在右側欄位中看到所有選定的埠。按一下「**OK**」以完成服務連線埠選取流程。

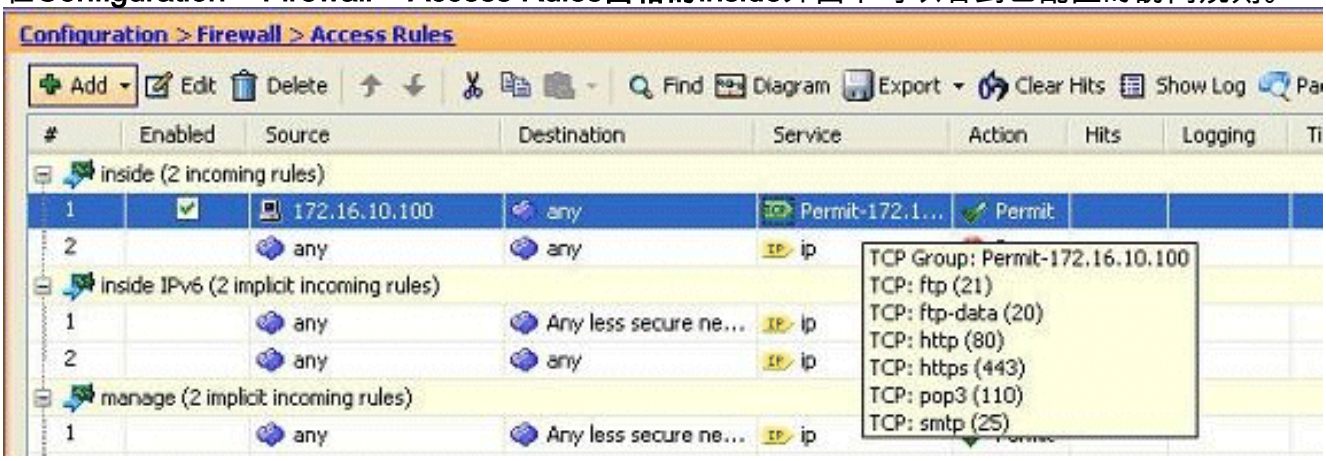


6. 您可以在此處看到已配置的TCP服務組。按一下「**OK**」（確定）。

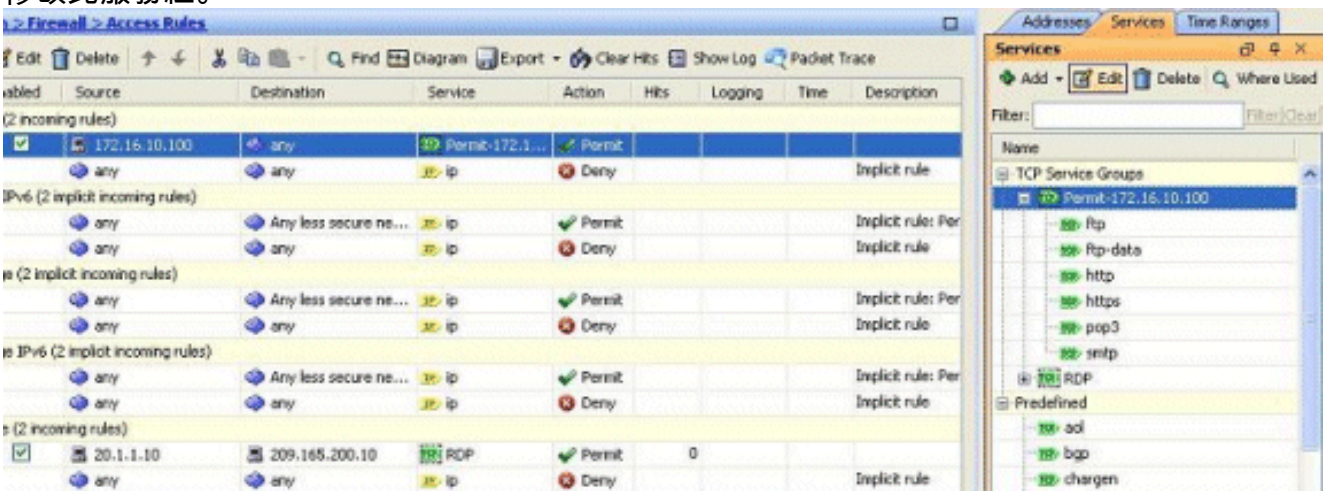

Browse Service
Add
Edit
Delete
Where Used
Filter:
Name
Protocol
Source Ports
Destination Ports
ICMP Type
Description
Permit-1...
tcp
ftp
tcp
default (1-65535)
21
ftp-data
tcp
default (1-65535)
20
http
tcp
default (1-65535)
80
https
tcp
default (1-65535)
443
pop3
tcp
default (1-65535)
110
smtp
tcp
default (1-65535)
25
RDP
tcp
Predefined
aol
tcp
default (1-65535)
5190
bgp
tcp
default (1-65535)
179
chargen
tcp
default (1-65535)
19
cifs
tcp
default (1-65535)
3020
citrix-ica
tcp
default (1-65535)
1494
ctiqbe
tcp
default (1-65535)
2748
daytime
tcp
default (1-65535)
13
discard
tcp
default (1-65535)
9
domain
tcp
default (1-65535)
53
echo
tcp
default (1-65535)
7
exec
tcp
default (1-65535)
512
Selected Service
Service ->
ip
OK



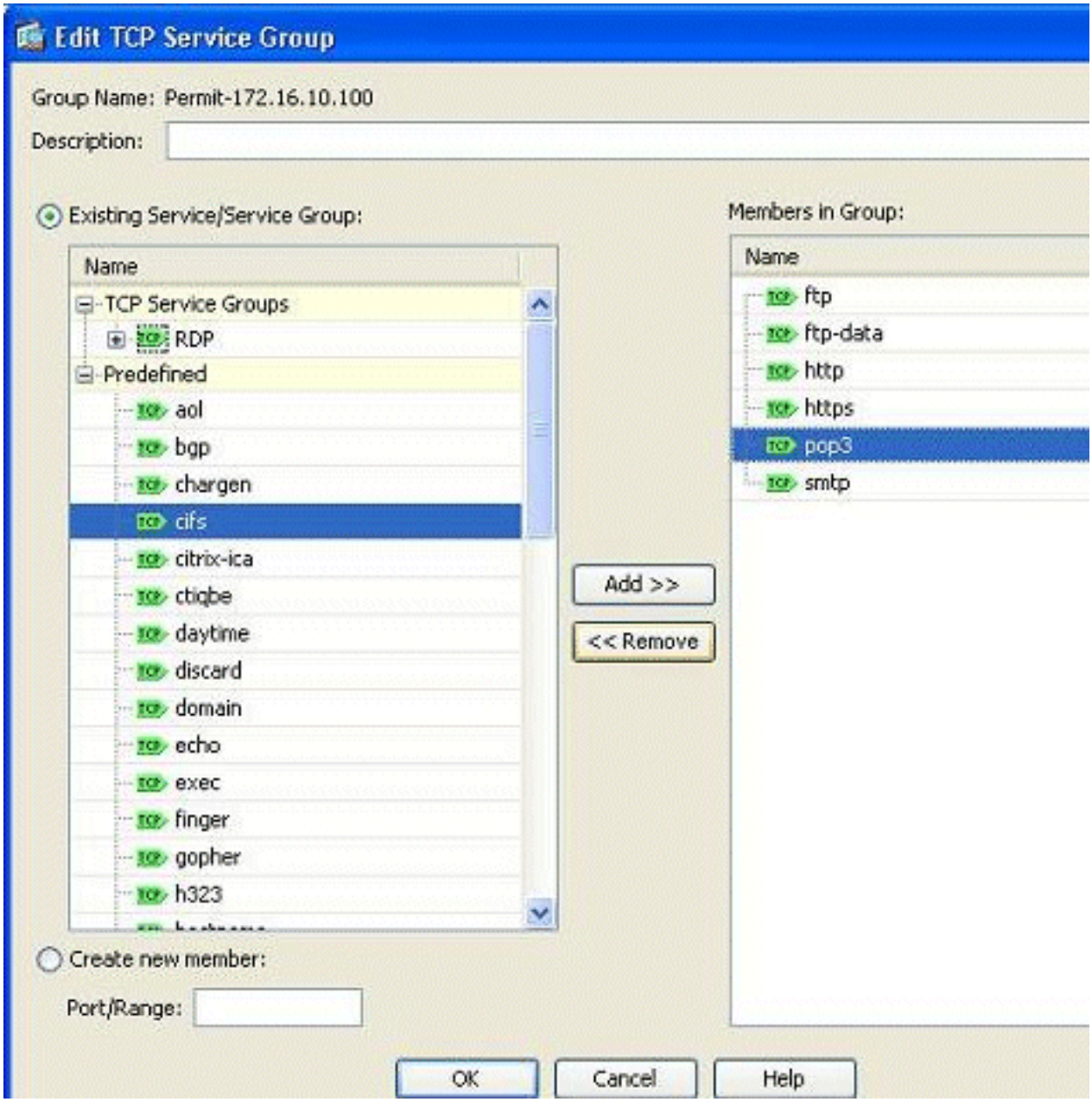
7. 按一下**OK**以完成設定。
8. 在**Configuration > Firewall > Access Rules**窗格的**inside**介面下可以看到已配置的訪問規則。



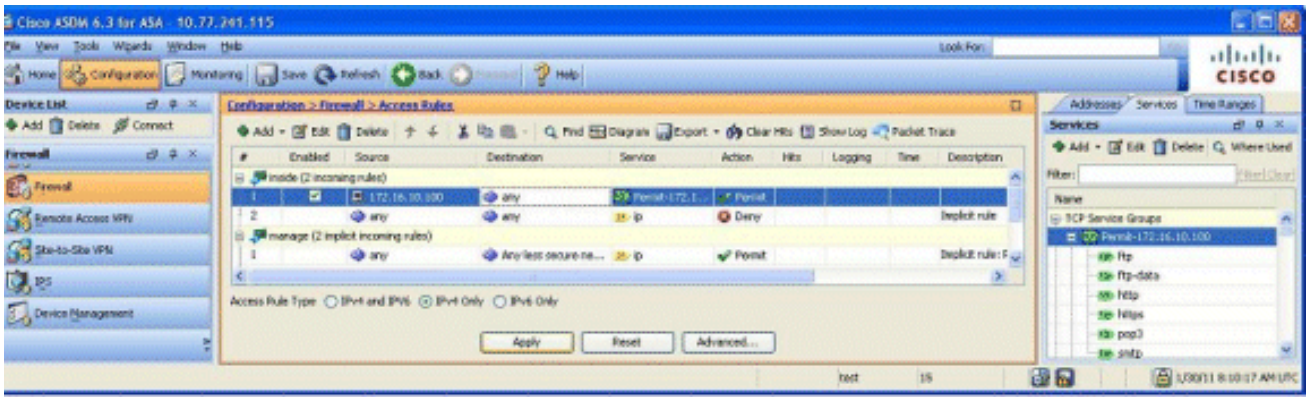
9. 為便於使用，您還可以直接在**Services**頁籤的右側窗格中編輯TCP服務組。按一下**Edit**以直接修改此服務組。



10. 它會再次重定向到「編輯TCP服務組」視窗。根據您的要求執行修改，然後按一下**OK**以儲存更改。



11. 此處顯示了ASDM的完整檢視：



這是等效的CLI配置：

```
object-group service Permit-172.16.10.100 TCP
 port-object eq ftp
 port-object eq ftp-data
 port-object eq www
```

```
 port-object eq https
 port-object eq pop3
 port-object eq smtp
!
access-list inside_access_in extended permit TCP host 172.16.10.100 any
    object-group Permit-172.16.10.100
!
access-group inside_access_in in interface inside
!
```

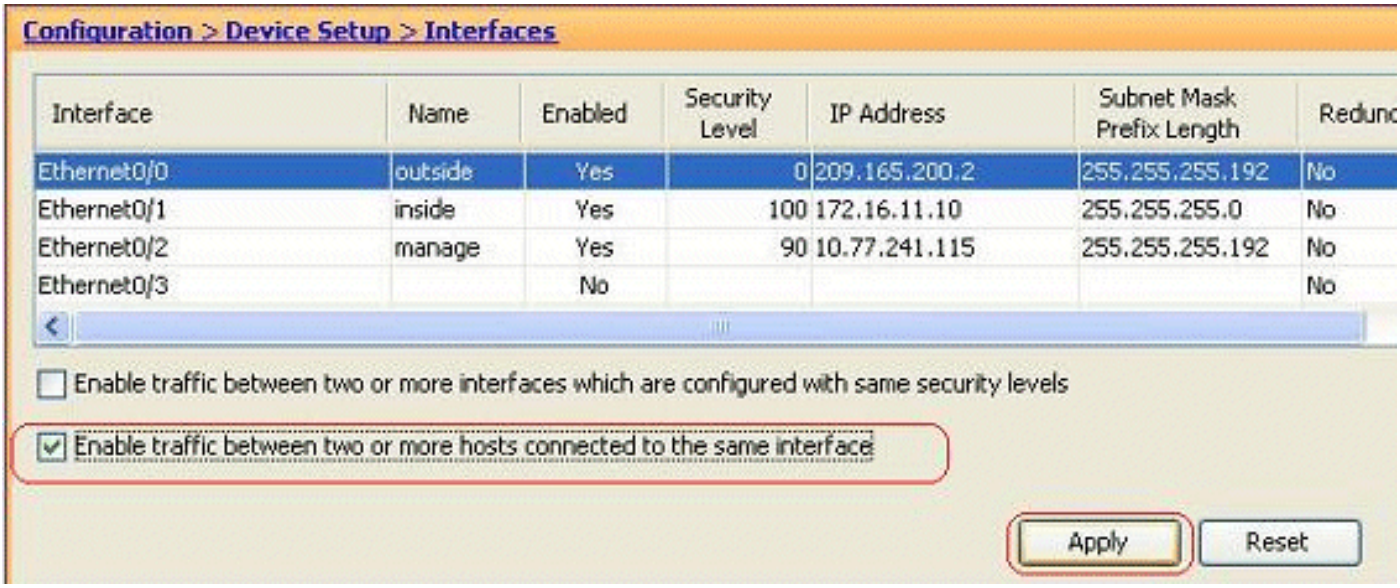
有關實施訪問控制的完整資訊，請參閱通過ASDM GUI新增或修改訪問清單。

允許具有相同安全級別的介面之間的流量

本節介紹如何在具有相同安全級別的介面內啟用流量。

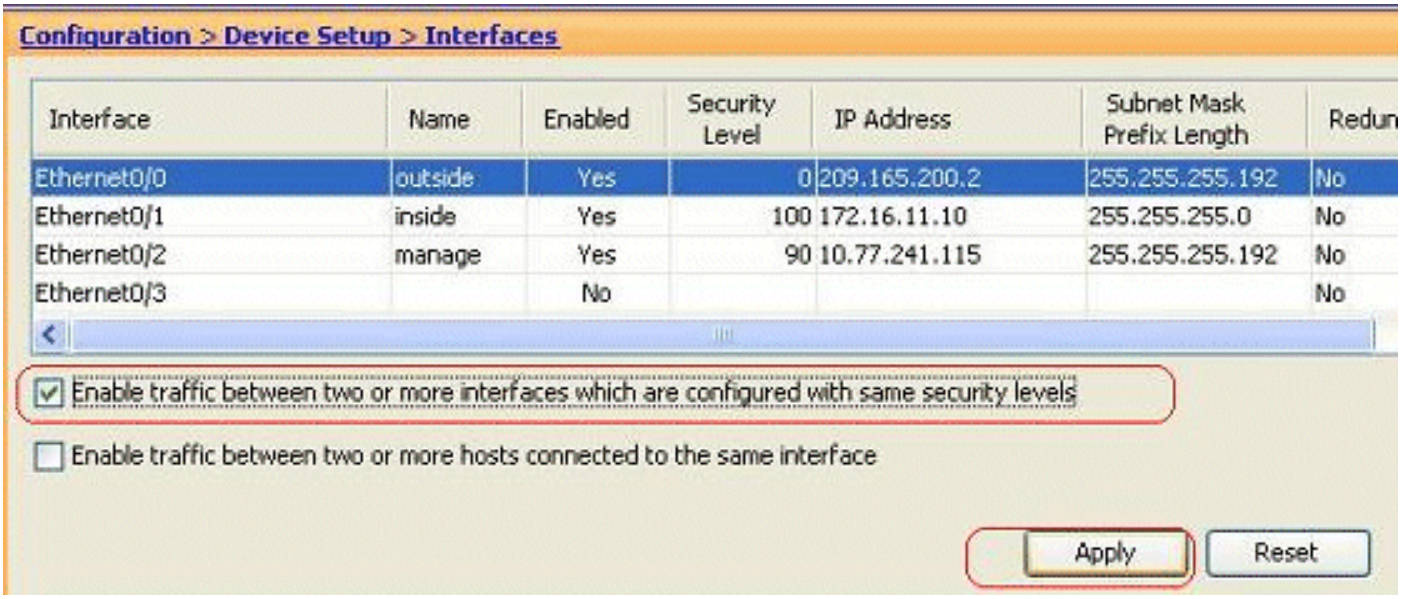
以下說明介紹了如何啟用介面內通訊。

這對於進入介面但隨後從同一介面路由出去的VPN流量很有用。在此案例中，VPN流量可能未加密，或者可能針對另一個VPN連線重新加密。前往**Configuration > Device Setup > Interfaces**，然後選擇**Enable traffic between two or more hosts connected to the same interface**選項。



以下說明介紹了如何啟用介面間通訊。

這對於允許具有同等安全級別的介面之間的通訊非常有用。前往**Configuration > Device Setup > Interfaces**，然後選擇**Enable traffic between two or more interfaces that configured with same security levels**選項。



這是這兩個設定的等效CLI:

```
same-security-traffic permit intra-interface
same-security-traffic permit inter-interface
```

允許不受信任的主機訪問受信任網路中的主機

這可以通過應用靜態NAT轉換和允許這些主機的訪問規則來實現。每當外部使用者想要訪問位於內部網路中的任何伺服器時，都需要進行此配置。內部網路中的伺服器將具有不可在Internet上路由的專用IP地址。因此，您需要通過靜態NAT規則將該私有IP地址轉換為公有IP地址。假設您有一個內部伺服器(172.16.11.5)。 為了讓此功能正常工作，您需要將此專用伺服器IP轉換為公共IP。本示例說明如何實施雙向靜態NAT以將172.16.11.5轉換為209.165.200.5。

此處未顯示有關通過實施訪問規則允許外部使用者訪問此Web伺服器的部分。為了便於理解，此處將顯示一個簡短的CLI片段：

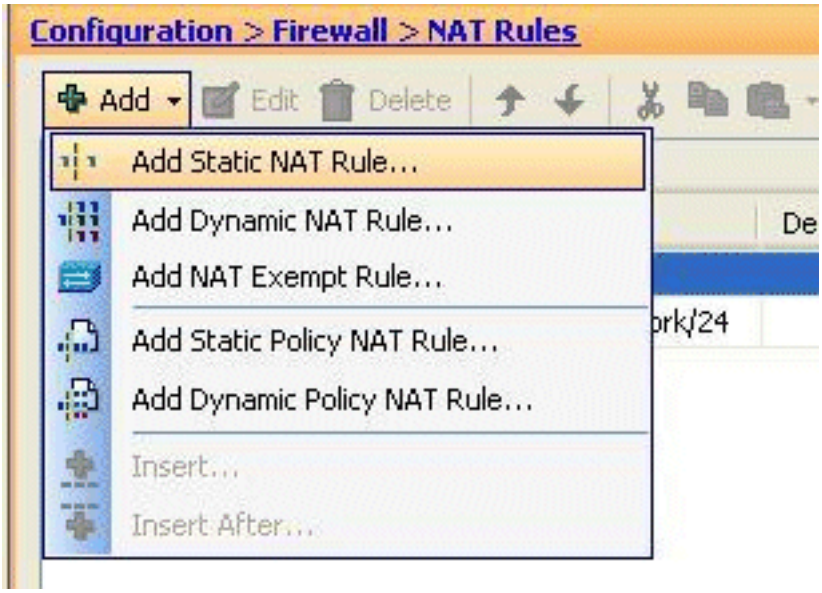
```
access-list 101 permit TCP any host 209.165.200.5
```

有關詳細資訊，請參閱通過ASDM GUI新增或修改訪問清單。

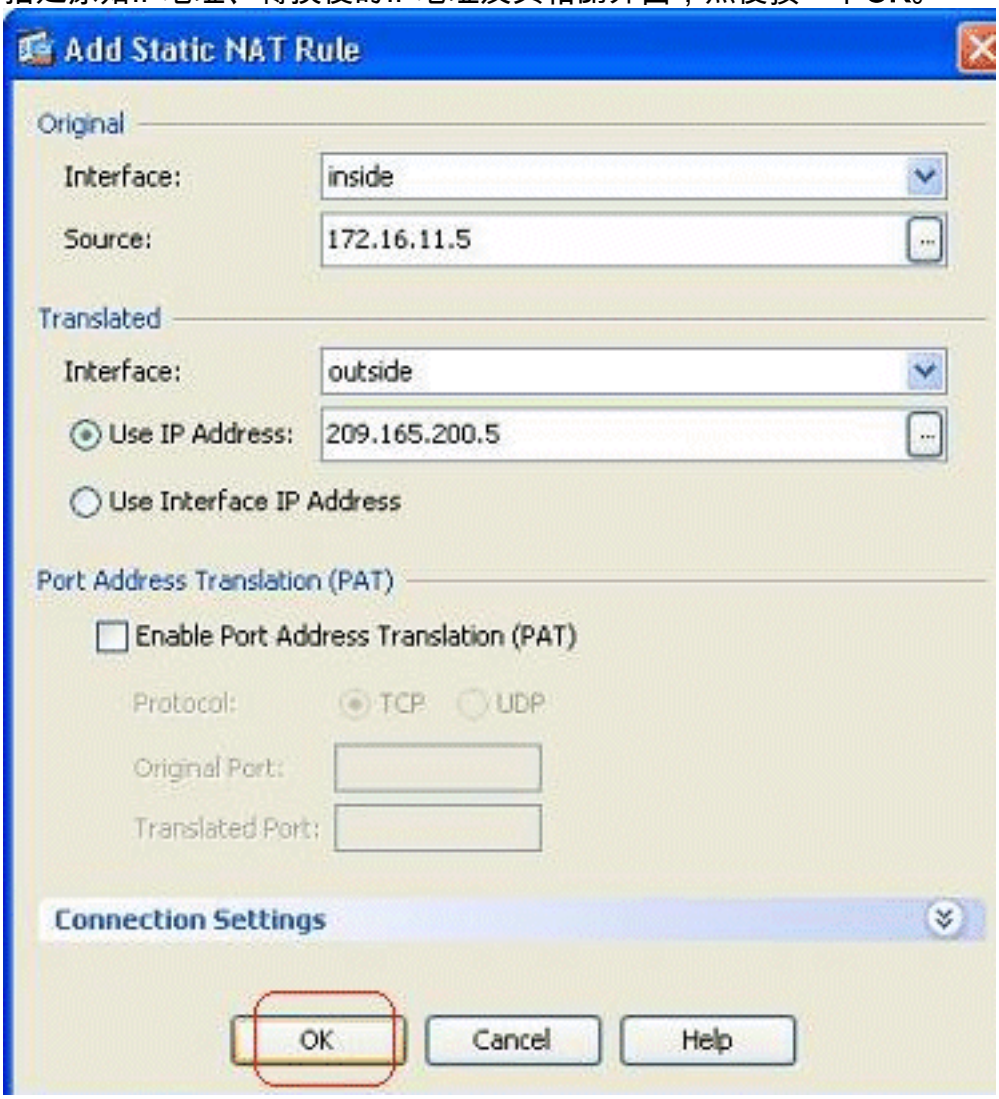
注意：指定關鍵字「any」允許來自外部世界的任何使用者訪問此伺服器。此外，如果沒有為任何服務埠指定該埠，則可在任何服務埠保持開啟狀態時訪問伺服器。實作時請務必小心，建議您將此許可權限製為單個外部使用者以及伺服器上的所需埠。

完成以下步驟以配置靜態NAT:

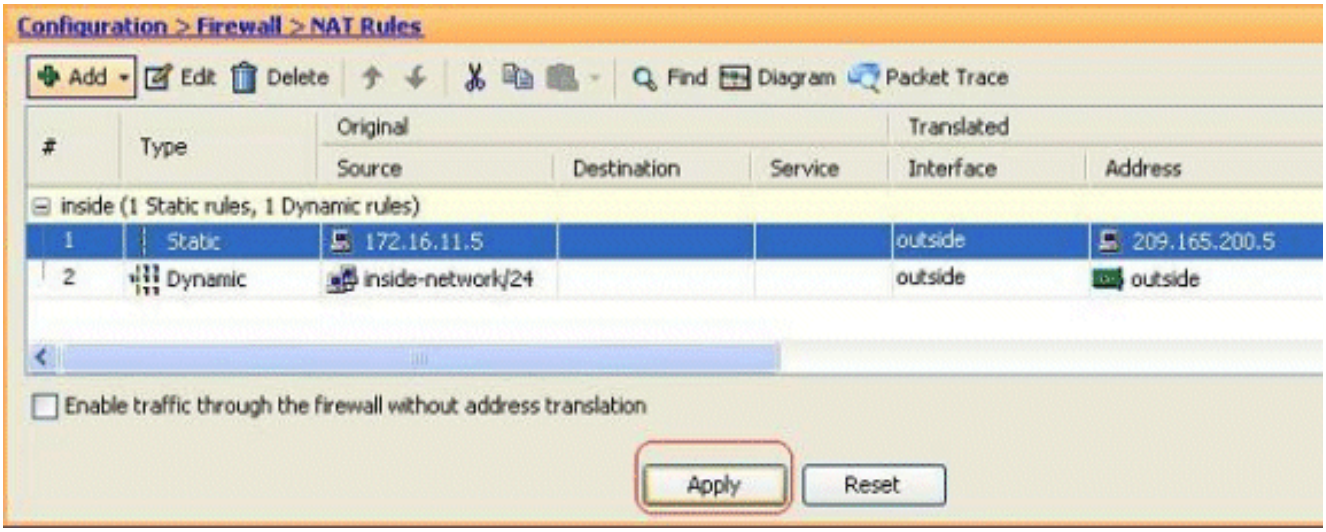
1. 轉至Configuration > **Firewall** > **NAT Rules**，按一下**Add**，然後選擇Add Static NAT Rule。



2. 指定原始IP地址、轉換後的IP地址及其相關介面，然後按一下**OK**。



3. 您可以在此處看到配置的靜態NAT條目。按一下**Apply**以將此命令傳送到ASA。



以下是此ASDM配置的簡短CLI示例：

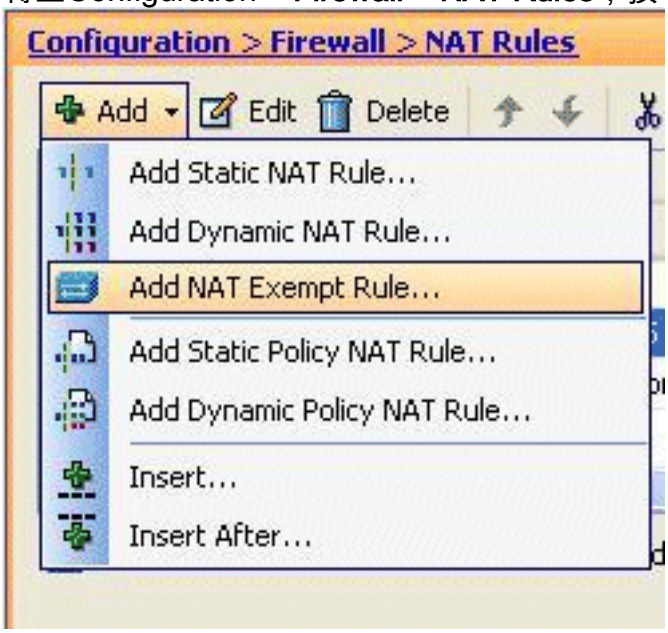
```
!
static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255
!
```

禁用特定主機/網路的NAT

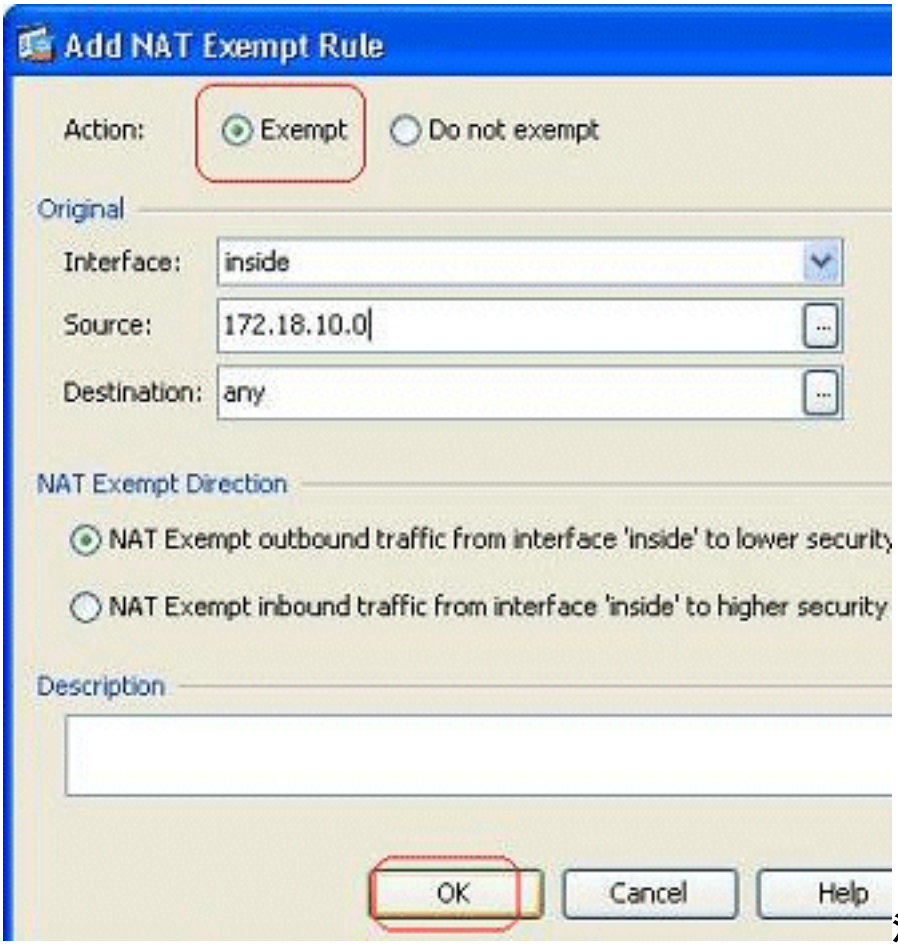
當需要將特定主機或網路免除NAT時，請新增NAT豁免規則以禁用地址轉換。這樣，轉換後的主機和遠端主機都可以發起連線。

請完成以下步驟：

1. 轉至Configuration > **Firewall > NAT Rules**，按一下**Add**，然後選擇Add NAT Exempt Rule。

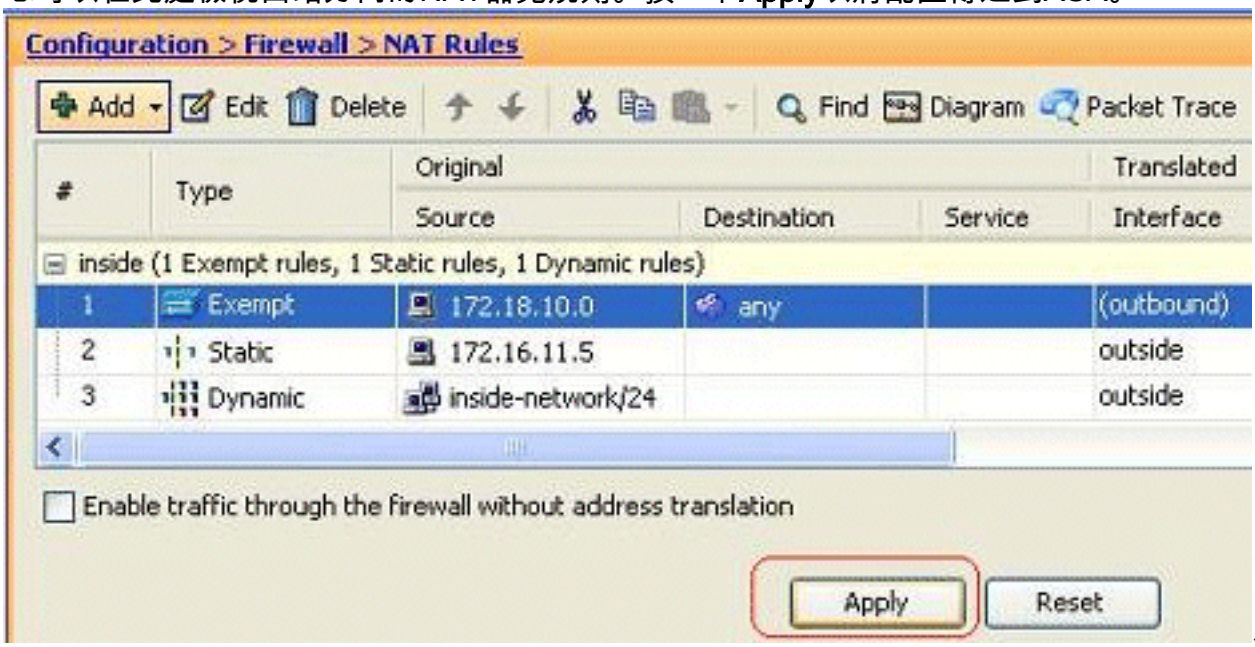


2. 這裡，內部網路172.18.10.0已免於地址轉換。確保已選擇**Exempt**選項。NAT Exempt Direction有兩個選項：到較低安全介面的出站流量到更高安全介面的入站流量預設選項用於出站流量。按一下「**OK**」以完成步驟。



注意：選擇**Do not exempt**選項時，該特定主機將不會被免除NAT，並且會使用「deny」關鍵字新增單獨的訪問規則。這有助於避免特定主機免除NAT，因為除這些主機之外的整個子網將免除NAT。

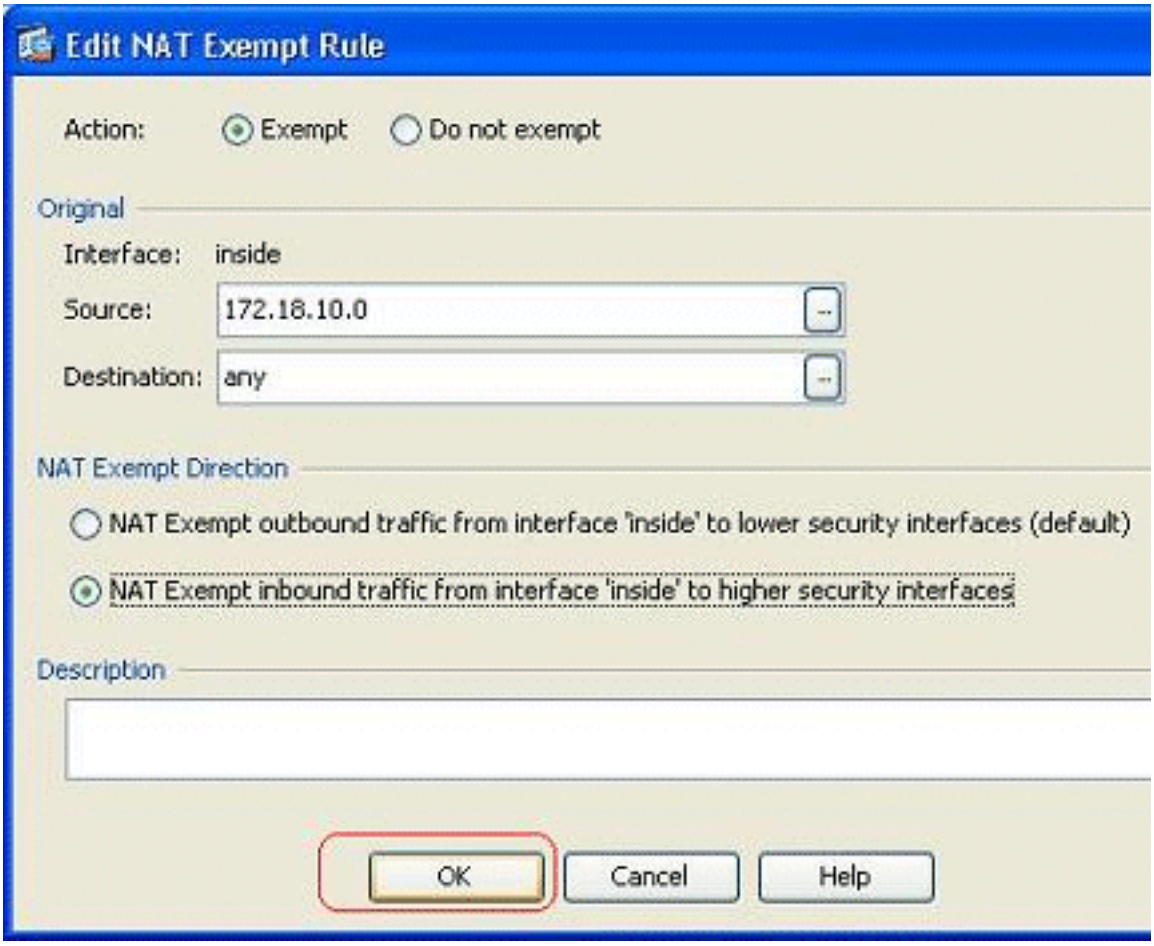
3. 您可以在此處檢視出站方向的NAT豁免規則。按一下**Apply**以將配置傳送到ASA。



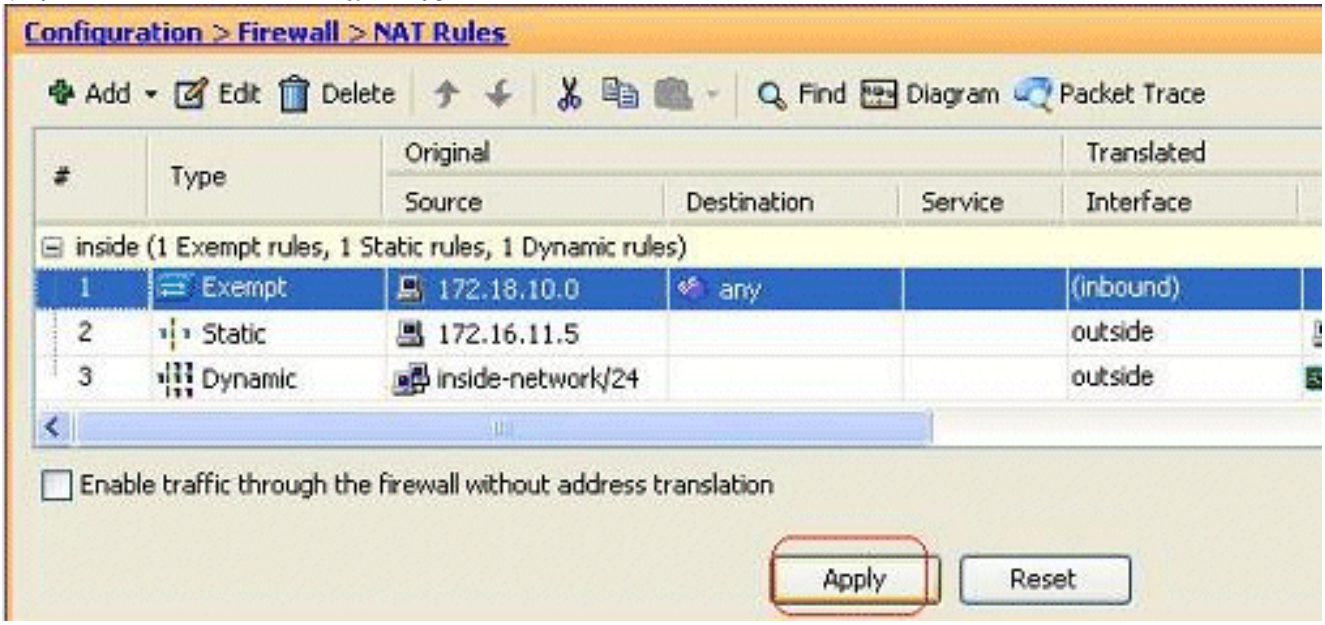
以下是供您參考的對等CLI輸出：

```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound
```

4. 在這裡，您可以看到如何編輯NAT豁免規則作為其方向。按一下**OK**使該選項生效。



5. 現在您可以看到方向已變更為*傳入*。

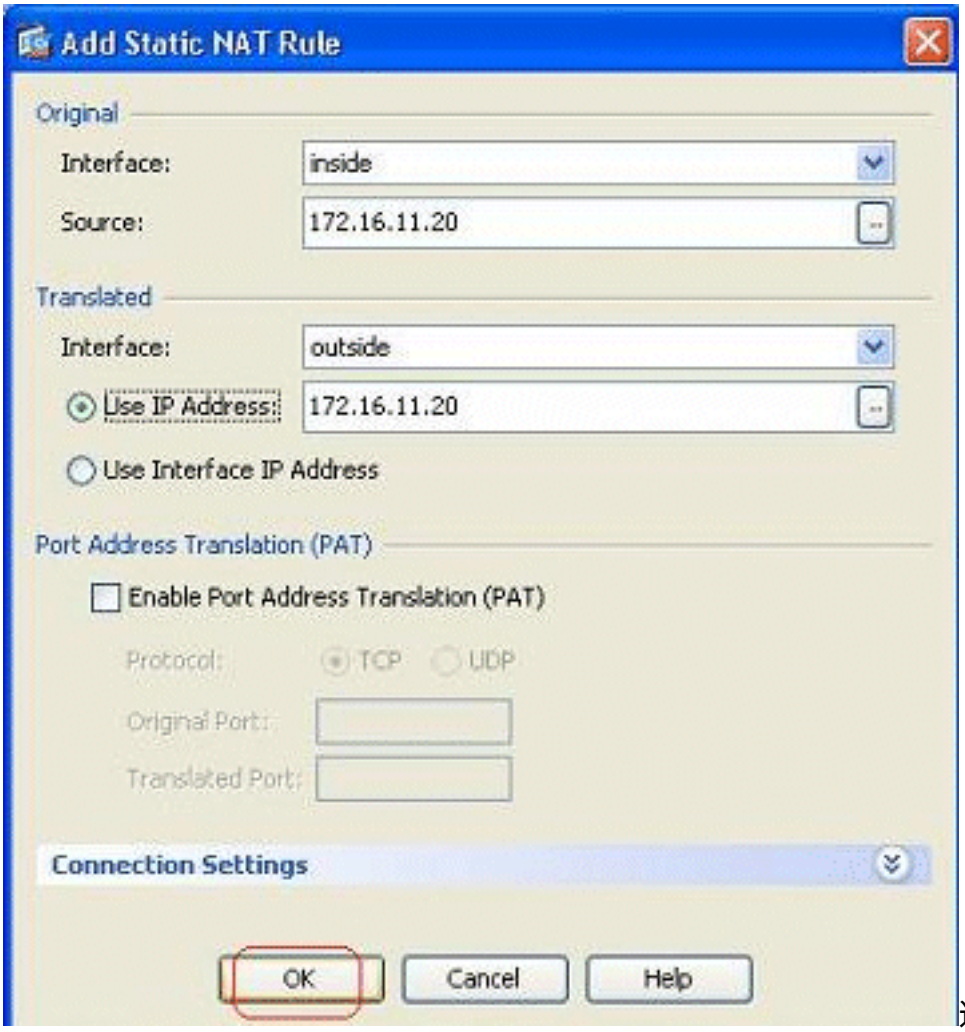


按一下**Apply**以將此CLI輸出傳送到ASA:

```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound outside
```

注意：從這裡可以看到，在**nat** 0命令的末尾新增了一個新的關鍵字(outside)。此功能稱為**外部NAT**。

6. 禁用NAT的另一種方法是實施身份NAT。身份NAT將主機轉換為相同的IP地址。以下是常規靜態身份NAT示例，其中主機(172.16.11.20)在從外部訪問時轉換為同一個IP地址。



這是等效的CLI輸出：

```
!
static (inside,outside) 172.16.11.20 172.16.11.20 netmask 255.255.255.255
!
```

連線埠重新導向（轉送）（含靜態）

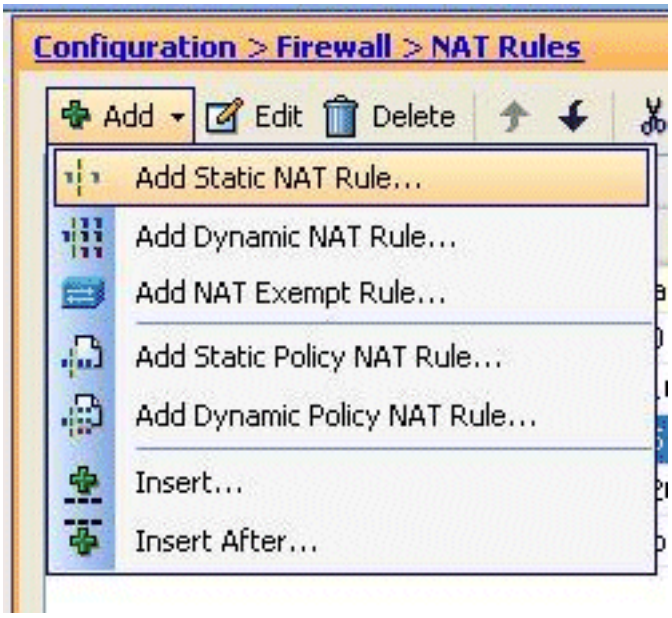
埠轉發或埠重定向是一項有用的功能，外部使用者可嘗試訪問特定埠上的內部伺服器。為此，內部伺服器（具有私有IP地址）將被轉換為公有IP地址，從而允許特定埠訪問。

在本例中，外部使用者想要訪問埠25上的SMTP伺服器209.165.200.15。這可通過兩個步驟完成：

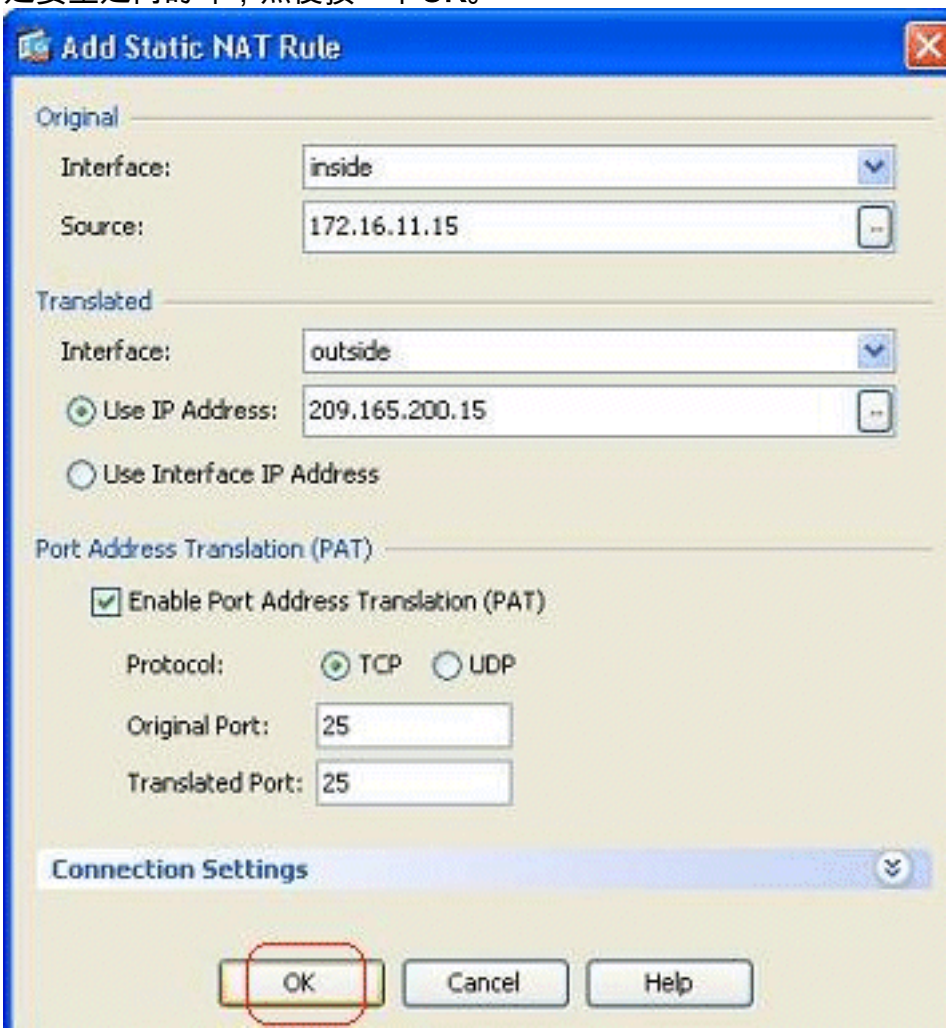
1. 將埠25上的內部郵件伺服器172.16.11.15轉換為埠25上的公共IP地址209.165.200.15。
2. 允許訪問埠25上的公共郵件伺服器209.165.200.15。

當外部使用者嘗試訪問埠25上的伺服器209.165.200.15時，此流量將重定向到埠25上的內部郵件伺服器172.16.11 15。

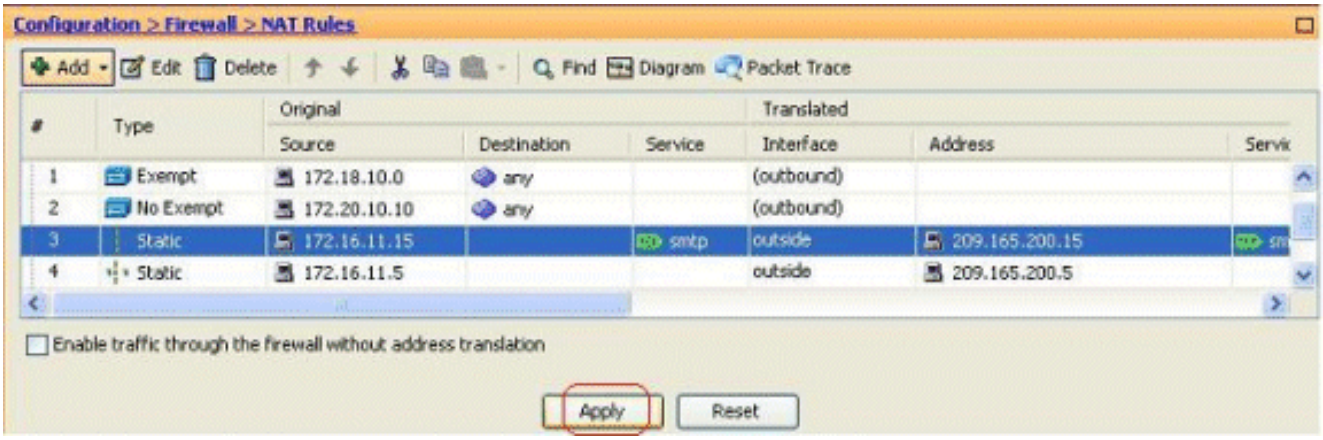
1. 轉至Configuration > **Firewall** > **NAT Rules**，按一下**Add**，然後選擇Add Static NAT Rule。



2. 指定原始源、轉換後的IP地址及其相關介面。選擇**Enable Port Address Translation(PAT)**，指定要重定向的埠，然後按一下**OK**。



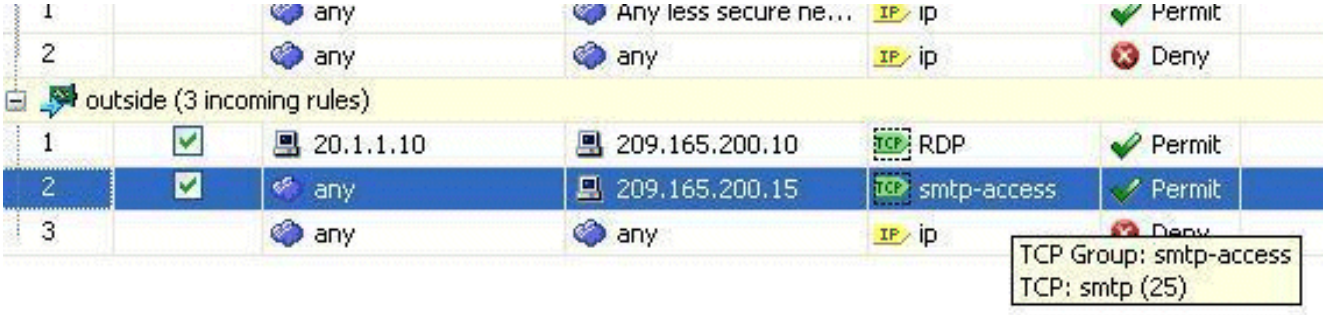
3. 配置的靜態PAT規則如下所示
：



這是等效的CLI輸出：

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
    255.255.255.255
!
```

4. 以下是允許外部使用者訪問位於209.165.200.15的公共smtp伺服器的訪問規則：



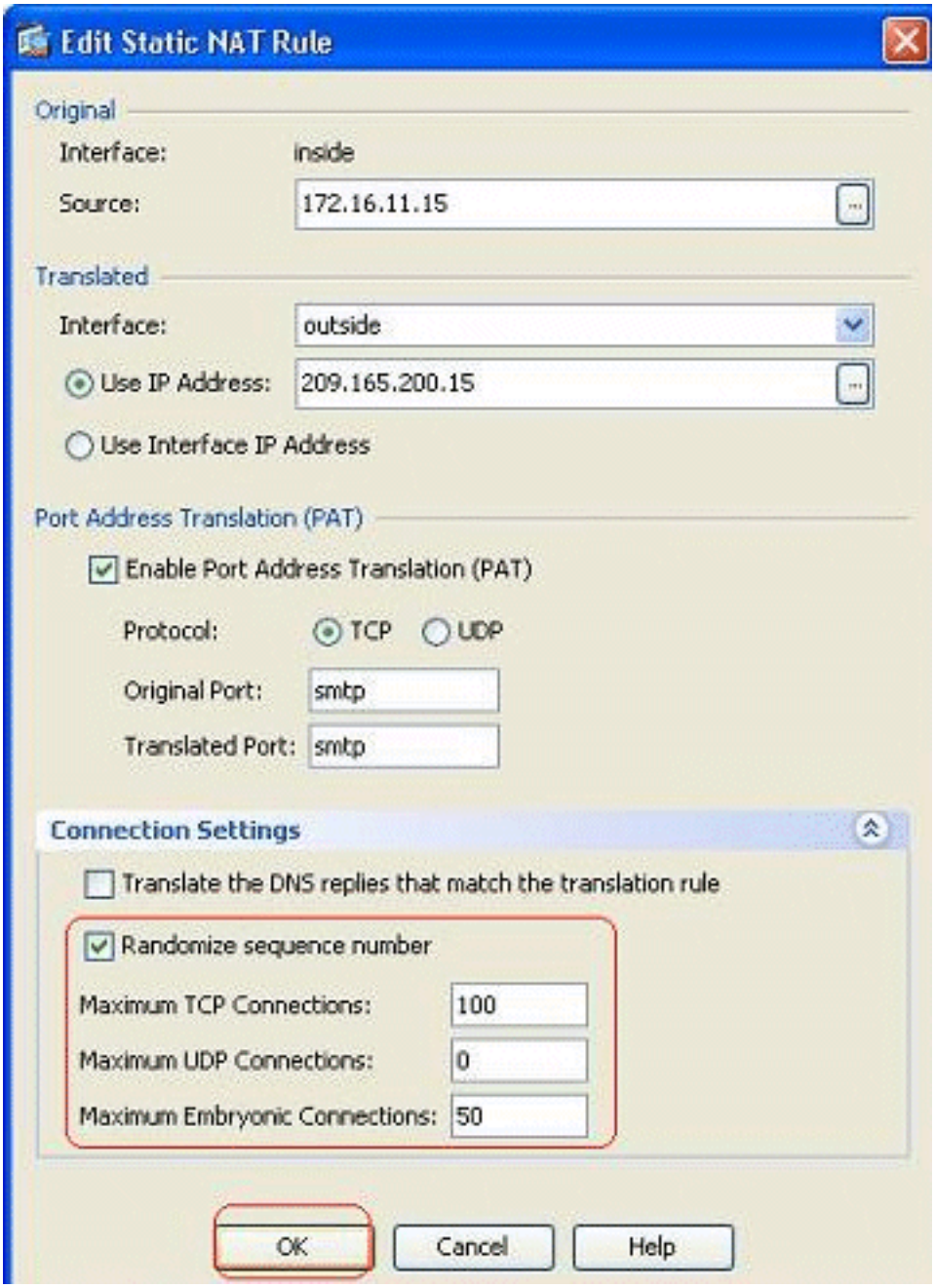
注意：確保使用特定主機，而不是在訪問規則的源中使用any關鍵字。

使用靜態限制TCP/UDP會話

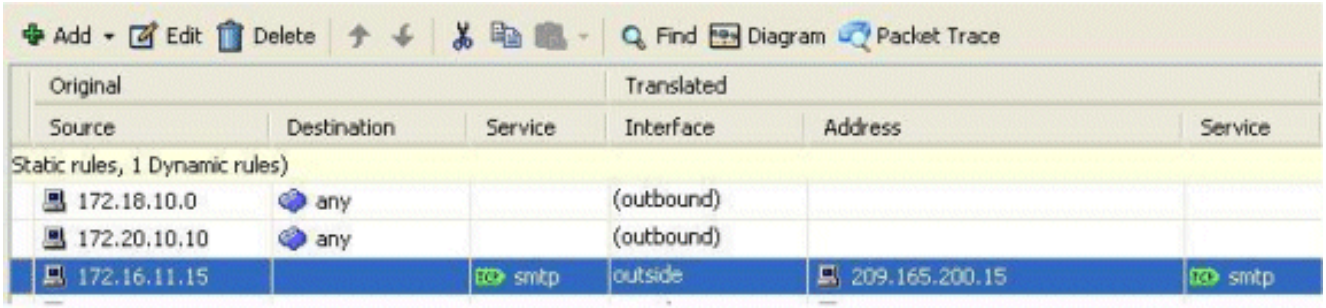
您可以使用靜態規則指定TCP/UDP連線的最大數量。您還可以指定初始連線的最大數量。半開連線是一種半開狀態的連線。其中大量資料將影響ASA的效能。限制這些連線將在某種程度上防止某些攻擊，如DoS和SYN。要完全緩解，您需要在MPF框架中定義策略，這超出了本文檔的範圍。有關此主題的其他資訊，請參閱減輕網路攻擊。

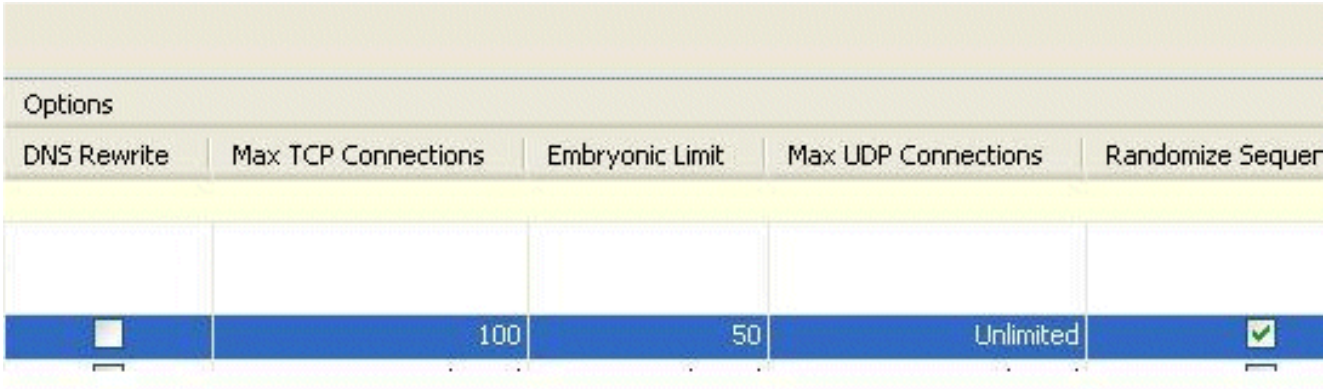
請完成以下步驟：

1. 按一下**Connection Settings**頁籤，並指定此靜態轉換的最大連線數。



2. 這些影象顯示了此特定靜態轉換的連線限制
:





這是等效的CLI輸出：

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
    255.255.255.255 TCP 100 50
!
```

時間型存取清單

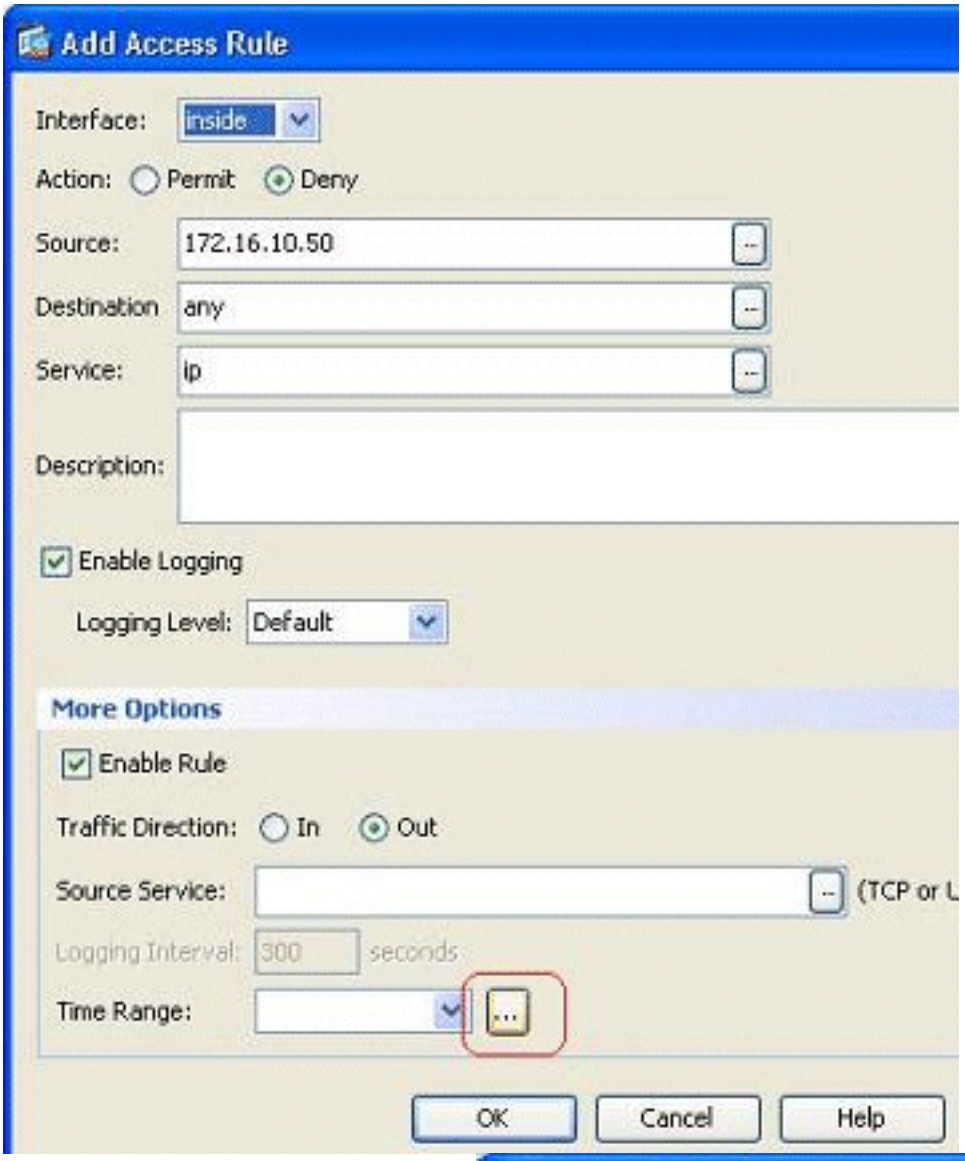
本節介紹如何使用ASDM實施基於時間的訪問清單。可以基於時間應用訪問規則。為了實施此功能，您需要定義一個時間範圍，指定按天/周/月/年計時。然後，您需要將此時間範圍繫結到所需的訪問規則。時間範圍可通過兩種方式定義：

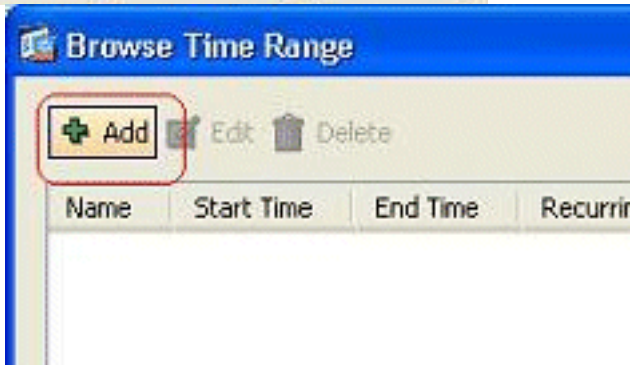
1. 絕對 — 定義包含開始時間和結束時間的時間段。
2. 定期 — 也稱為定期。定義以指定間隔發生的時間段。

注意：在配置時間範圍之前，請確保已為ASA配置了正確的日期/時間設定，因為此功能使用系統時鐘設定實施。使ASA與NTP伺服器同步將產生更好的結果。

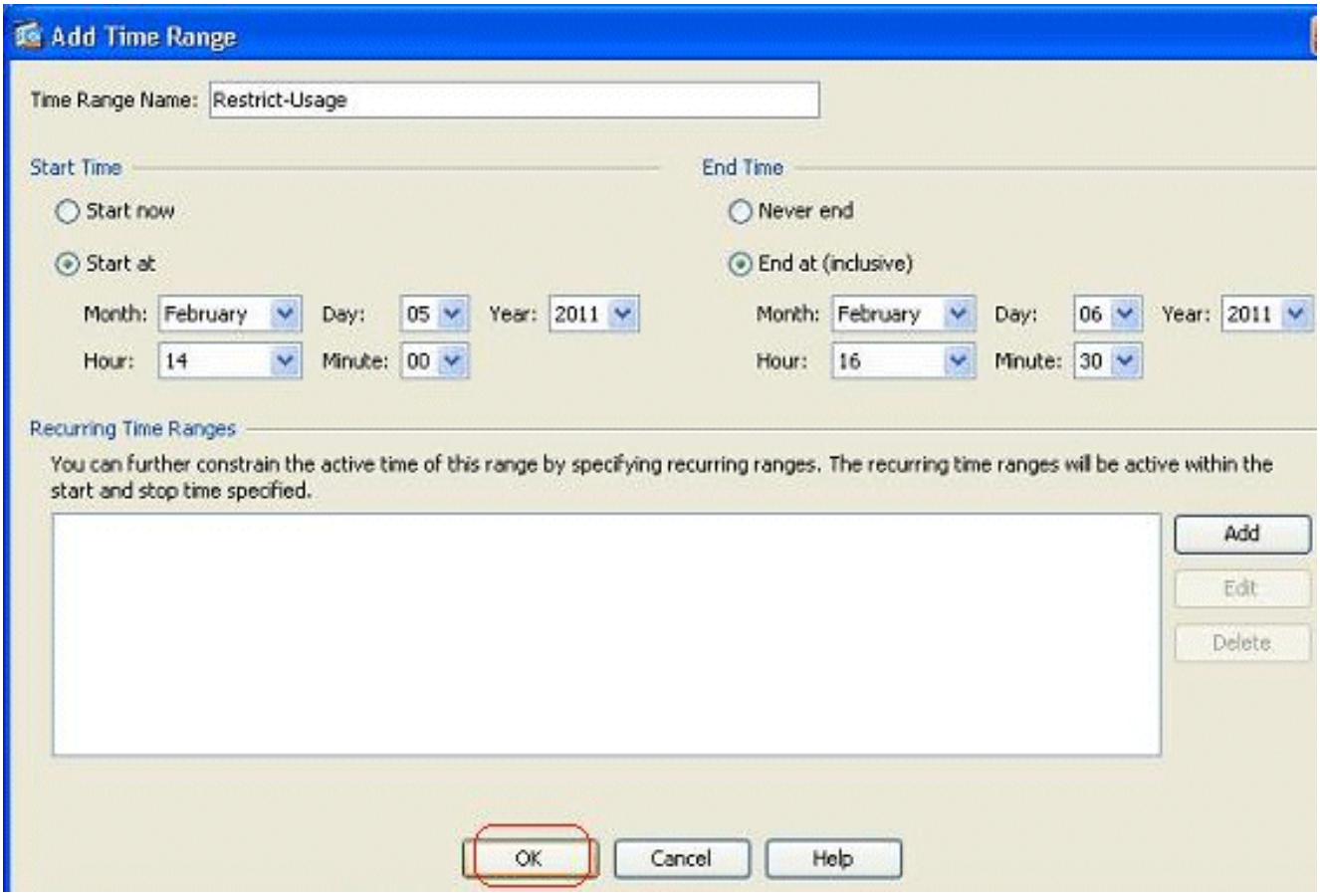
完成以下步驟，以便通過ASDM配置此功能：

1. 定義訪問規則時，按一下Time Range欄位中的**Details**按鈕。

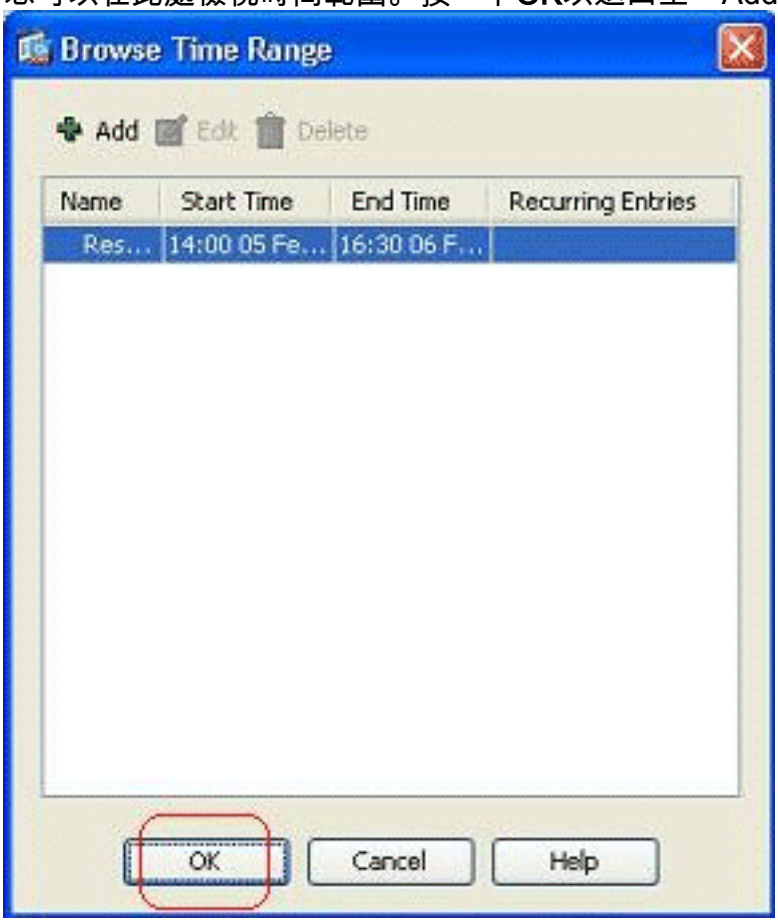




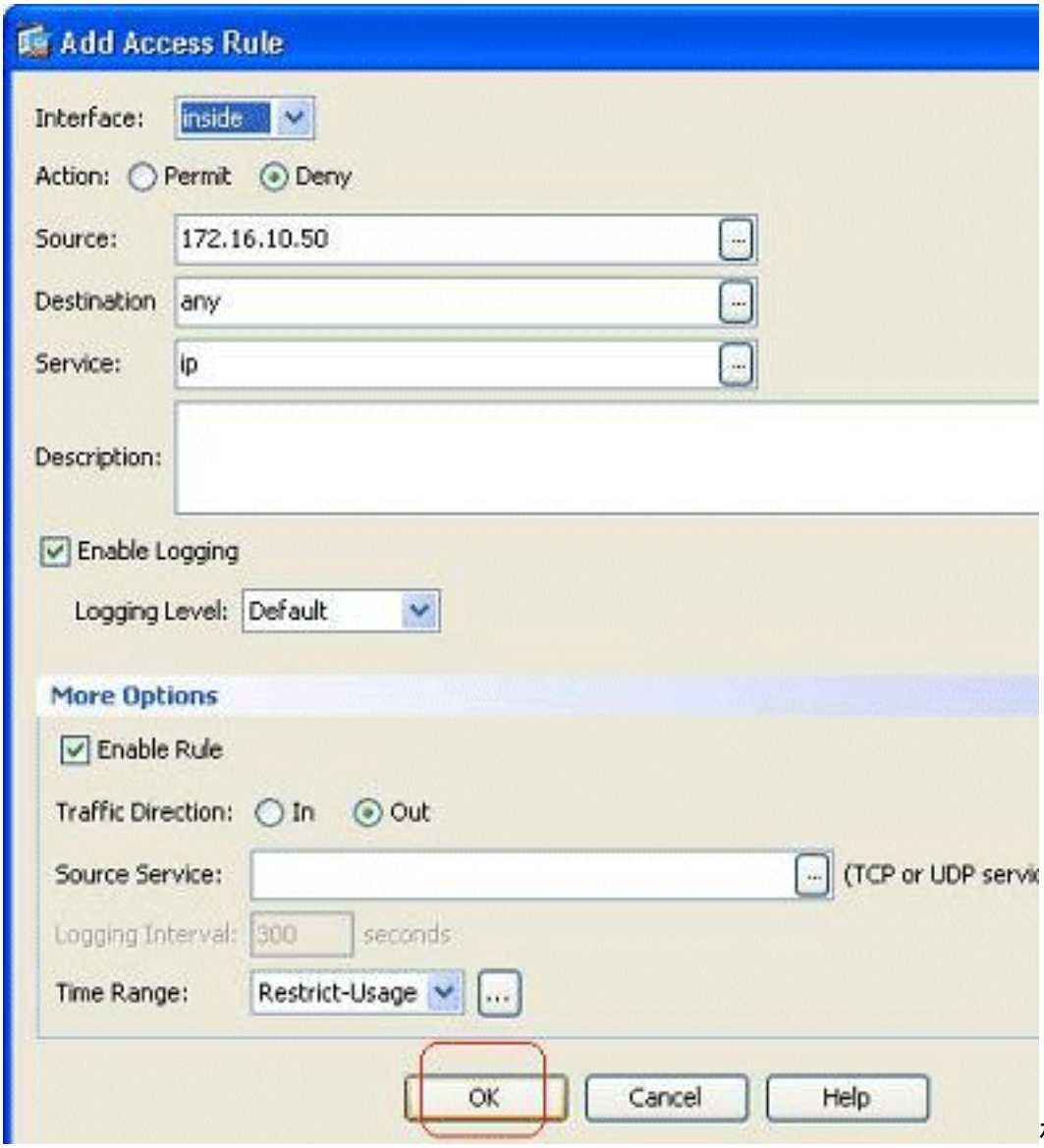
2. 按一下**Add**以建立新的時間範圍。
3. 定義時間範圍的名稱，並指定開始時間和結束時間。按一下「**OK**」（確定）。



4. 您可以在此處檢視時間範圍。按一下**OK**以返回至「Add Access Rule」視窗。



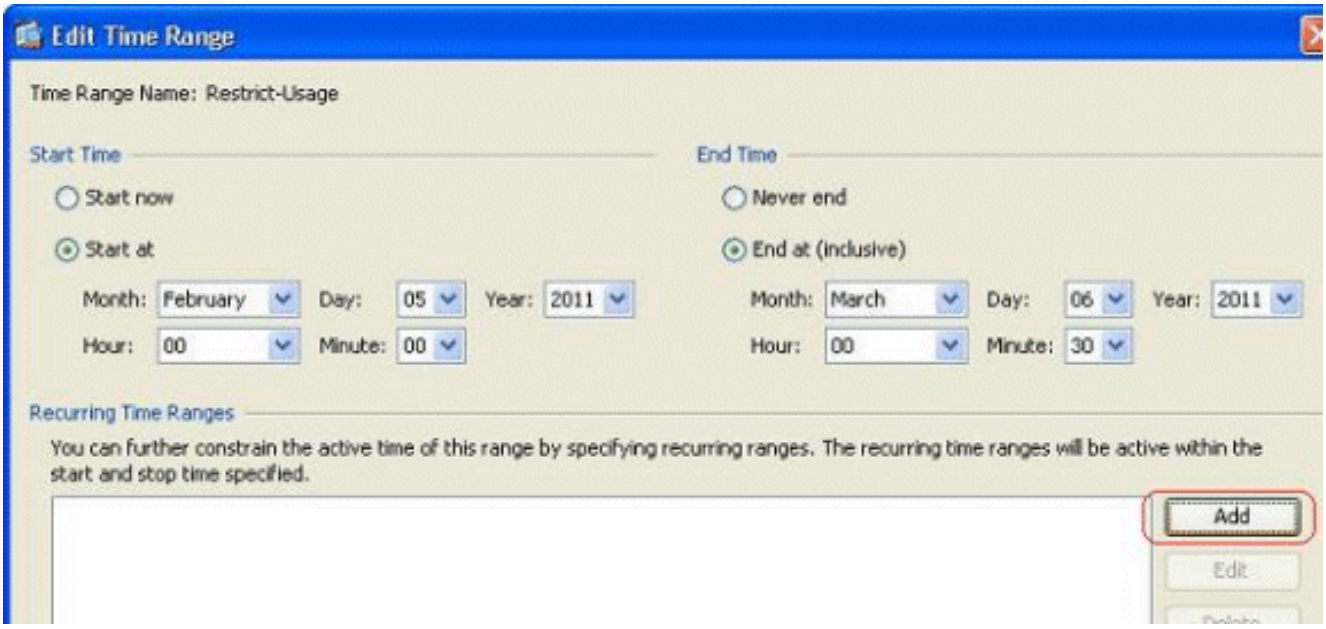
5. 現在您可以看到Restrict-Usage時間範圍已繫結到此訪問規則。



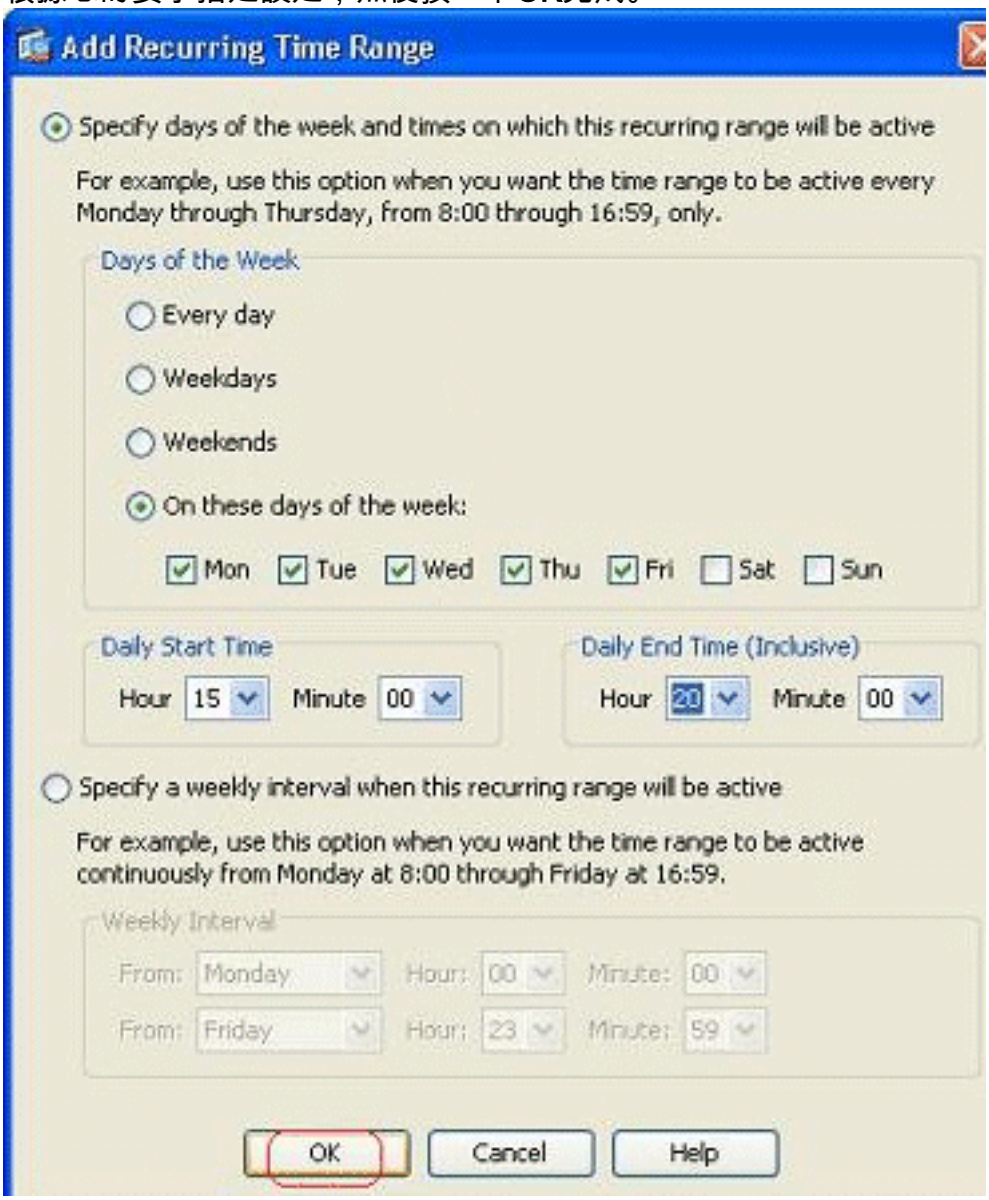
根據此訪問規則配置，位於172.16.10.50的使用者被限制使用從2011年2月5日下午2點到2011年2月6日下午4.30點之間的任何資源。這是等效的CLI輸出：

```
time-range Restrict-Usage
 absolute start 14:00 05 February 2011 end 16:30 06 February 2011
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

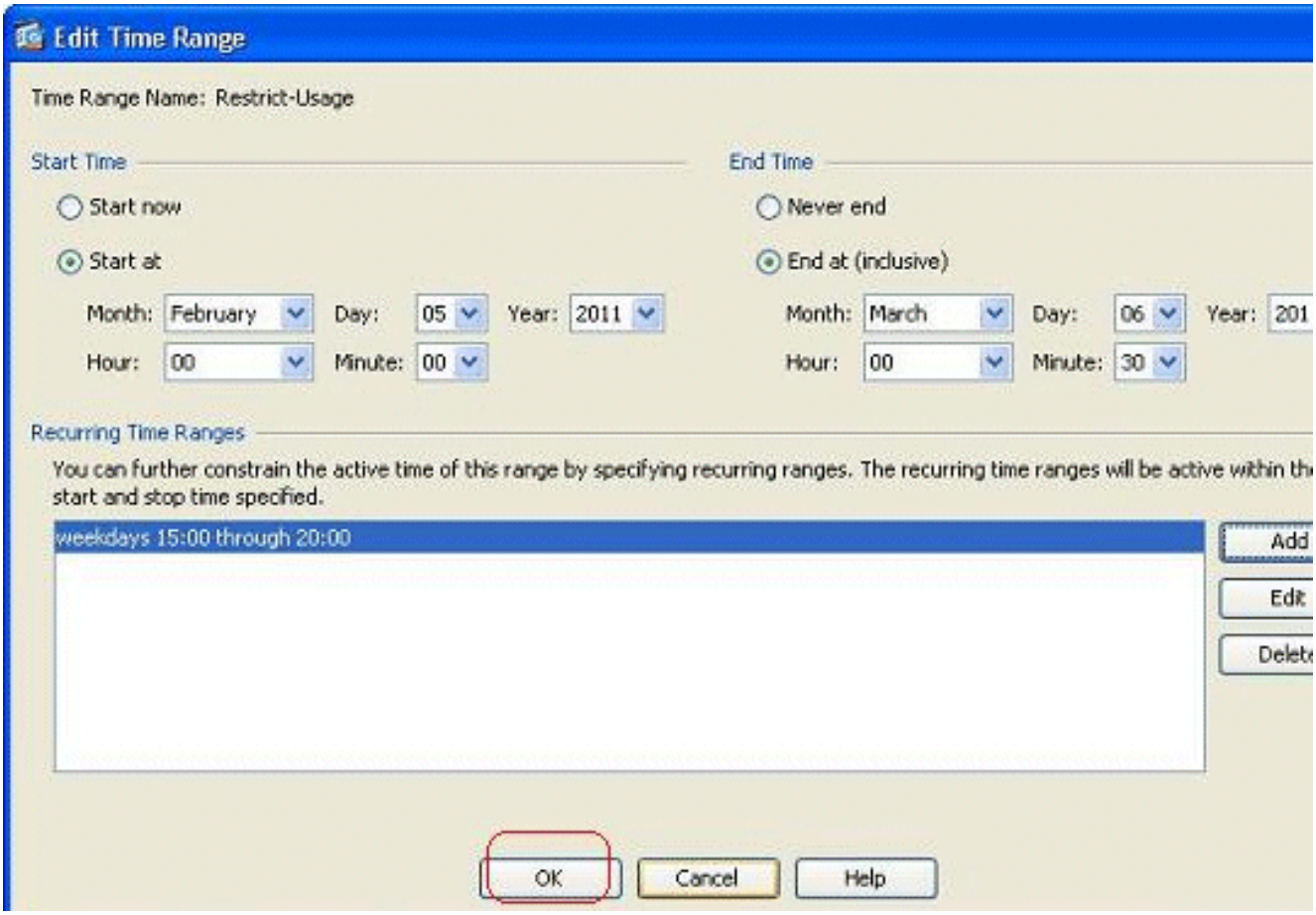
6. 以下示例說明如何指定循環時間範圍。按一下Add以定義定期時間範圍。



7. 根據您的要求指定設定，然後按一下**OK**完成。



8. 按一下**OK**以返回到「時間範圍」視窗。



根據此配置，從172.16.10.50上的使用者被拒絕在除星期六和星期日外的所有工作日（從下午3點到晚上8點）訪問任何資源。

```
!
time-range Restrict-Usage
 absolute start 00:00 05 February 2011 end 00:30 06 March 2011
 periodic weekdays 15:00 to 20:00
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

註：如果time-range命令同時指定了絕對值和週期值，則只有在達到絕對開始時間後才會評估periodic命令，而在達到絕對結束時間後不會進一步評估。

相關資訊

- Cisco ASA文檔頁面
- 技術支援與文件 - Cisco Systems